Acknowledgements

This study was requested by the American Association of State Highway and Transportation Officials (AASHTO), and conducted as part of National Cooperative Highway Research Program (NCHRP) Project 20-59(5). The NCHRP is supported by annual voluntary contributions from the state Departments of Transportation. Project 20-59 is intended to fund quick response studies on behalf of the AASHTO Security Task Force. The report was prepared by Douglas B. Ham and Stephen Lockwood of Parsons Brinckerhoff with the support of Leo Gonnering of Parsons Brinckerhoff and Bhasker (Bob) Tripathi of SAIC. The work was guided by a task group that included David S. Ekern, Anthony R. Kane, Vincent Pearce, Ray Purvis, Mary Lou Ralls, and Terry Simmonds. The project was managed by S. A. Parker, CRP Senior Program Officer.

Disclaimer

The opinions and conclusions expressed or implied are those of the research agency that performed the research and are not necessarily those of the Transportation Research Board or its sponsors. This report has not been reviewed or accepted by the Transportation Research Board's Executive Committee or the Governing Board of the National Research Council.

Security

Some material from the original draft report regarding blast/structures interaction and countermeasures has been redacted from this edition and is available only through AASHTO.
# TABLE OF CONTENTS

**Forward: How to Use this Document** ................................................................. iv

**Executive Summary** .......................................................................................... v

**Part I. Highway-Related Security Program Overview** ................................. 1

1. **Introduction** ..................................................................................................... 1  
   1.1 AASHTO Reauthorization Security Policy ....................................................... 1  
   1.2 Focus of this Report ....................................................................................... 2  
   1.3 Focus on Terrorism and Weapons of Mass Destruction (WMD) ............... 2

2. **Development of the Program Estimates** ......................................................... 5  
   2.1 AASHTO Security Programs .......................................................................... 5  
   2.1.1 Caveats and Uncertainties ....................................................................... 6  
   2.1.2 Program for Protection of Critical Mobility Assets ............................... 7  
   2.1.3 Program for Enhancement of Traffic Management Capabilities .......... 8  
   2.1.4 Program for Improvement of State DOT Emergency Response ......... 9
   2.2 Dual Use Benefits ......................................................................................... 11  
   2.3 Total Security Investment Needs ................................................................. 11

**Part II. Security Programs** .............................................................................. 14

3. **Program for Protection of Critical Mobility Assets** .................................... 14  
   3.1 Risk Management Strategy .......................................................................... 14  
   3.2 Threat Assumptions ..................................................................................... 14  
   3.3 Definition of “Critical” Highway System Assets ...................................... 17  
   3.4 Bridge and Tunnel Vulnerability ................................................................. 21  
   3.5 Bridge and Tunnel Countermeasures and Costs ....................................... 24  
   3.6 Needed Research Program ......................................................................... 30

4. **Program for Enhancement of Traffic Management Capabilities** .......... 30  
   4.1 Needed Capabilities ..................................................................................... 30  
   4.2 Highway Management Systems Deployment ............................................ 31  
   4.3 Highway Management Systems Strategic Control ..................................... 33  
   4.4 Program Costs ............................................................................................. 34

5. **Program for Improvement of State DOT Emergency Response** ............ 35  
   5.1 Expanding Role of State DOTs in Emergency Response ......................... 36  
   5.2 Fundamental Emergency Management Thinking ....................................... 37  
   5.3 Identified Shortcomings .............................................................................. 38  
   5.4 An Emergency Response Capacity-Building Program for State DOTs .... 40  
   5.5 Program Costs ............................................................................................. 42  
   5.6 Cost Analysis Assumptions ......................................................................... 43
6. Appendix.................................................................................................................. 46
A. List of Acronyms..................................................................................................... 46
LIST OF FIGURES

Figure 1: Vehicle Bomb Explosion Effects ................................................................. 17

LIST OF TABLES

Table 1: Annual and Six-Year Total Costs Summary for Highway-Related Security Programs ................................................................. ix
Table 2: WMD Characteristics and Effects on Infrastructure and Other Targets ........ 3
Table 3: Possible Similarities and Dissimilarities between Terrorist WMD and Natural Disasters ................................................................. 4
Table 4: National Highway-Related Security Program Cost Structure ................. 12
Table 5: Annual and Six-Year Total Costs Summary for Highway-Related Security Programs ........................................................................ 13
Table 6: Determination of "Critical" Bridges ................................................................. 20
Table 7: Explosive Attack Scenarios ......................................................................... 22
Table 8: Bridge and Tunnel Countermeasures ............................................................ 25
Table 9: Six-Year Total Costs for Bridge Retrofit ..................................................... 26
Table 10: Six-Year Costs for Tunnel Retrofit ............................................................. 30
Table 11: Strategy Assumptions for National Highway Emergency Management and Monitoring System ......................................................... 34
Table 12: Six-Year Total Costs for Enhancement of Traffic Management Capabilities . 34
Table 13: Emergency Response Capacity-Building Program .................................. 40
Table 14: Annual and Six-Year Total Costs for Improvement of State DOT Emergency Response Capabilities ......................................................... 43
Forward: How to Use this Document

This report further develops and refines the concepts and costs presented in the security policy component of the American Association of State Highway and Transportation Officials (AASHTO) Reauthorization proposals and dimensioned in the AASHTO 2002 Bottom Line Report. The three program areas have been prepared to provide support for the rationale, components, and costs of the proposed programs. Towards this end, the program assumptions and national costs have been developed using national system inventories, “average” conditions, and generic unit costs.

The report targets federal, state, regional, and metropolitan transportation planners and policy makers. Users of the document may either examine the three program areas – protecting critical mobility assets, enhancing emergency routes, and improving emergency response – as an integrated whole, or utilize them individually. Users are free to adjust the cost assessment data in the report to accommodate specific infrastructure scenarios.

Casual readers of this report should, as a minimum, consult the Executive Summary. High-level managers involved in transportation security planning will want, additionally, to review Part I of the report, which examines the three program areas and identifies key capital and O&M (operating and maintenance) costs associated with national implementation of each program. Staff responsible for budget development will also want to consult Part II of this report, which provides important information on the assumptions, unit costs, etc. used in preparing the cost estimates for each program area. In addition to the materials presented in this report, the authors have prepared an “estimator tool”, comprised of a series of Excel spreadsheets, which can be used to adapt the national budget estimates to specific user-defined geographic areas; program area assumptions are modifiable to accommodate the transportation security requirements of a particular state, region, or locality. The estimator tool is available directly from AASHTO.

Users of this document should bear in mind that safeguarding the nation’s transportation infrastructure from threats of terrorism is still in its infancy. Consequently, the concepts and costs offered in this report represent best, “first-cut” approaches to areas still very much in development.
Executive Summary

The specter of international terrorists armed with weapons of mass destruction (WMD) establishes a new context for transportation security policy and planning. This context includes not only an expanded threat matrix (in the form of explosive, chemical, biological, and radiological weapons), but also the potential of a variety of delivery mechanisms, combinations, and environmental settings.

Among surface transportation’s modal systems, the nation’s highway infrastructure is relatively robust and redundant. Nevertheless, the consequences – both direct and indirect – of an attack on critical links could be significant. There are certain contexts across the United States in which the loss of key links could have major economic and mobility impacts and result in immediate loss of life. Furthermore, as demonstrated on September 11, 2001, highway systems can play a vital role in response to terrorist incidents via their evacuation and emergency access roles.

This study, conducted under the auspices of the Transportation Security Task Force of the American Association of State Highway and Transportation Officials (AASHTO), examines three key security planning program areas:

- Protecting critical mobility assets,
- Enhancing traffic management capabilities, and
- Improving state DOT (Department of Transportation) emergency response capabilities.

Total costs for the proposed initiatives, including capital investment and operations and maintenance expenses during the TEA-21 (Transportation Equity Act for the 21st Century) six-year reauthorization period, are estimated at $10.5 billion.

Key elements of the three security planning initiatives are summarized below. Note that in addition to the national security benefits offered by the prospective program, investment in the initiatives is expected to yield important non-security gains, including (1) safety improvements to bridges and tunnels; (2) enhanced operational capabilities of the surface transportation network; and (3) upgraded emergency response and management capabilities for state DOTs.

Protecting Critical Mobility Assets

The principal threat against highway physical assets is explosive attacks on key links such as bridges, interchanges, and tunnels. Facilities most vulnerable to disruptions are those playing important regional and strategic roles, the loss of which would be maximally disruptive and involving greater replacement challenges. On a nationwide basis, approximately 450 bridges and 50 tunnels meet relevant criteria as critical assets. While full asset protection is not feasible, reasonable program objectives include the
deterrence of terrorist attacks by (1) adding new and clearly visible security features and reducing vulnerabilities, and (2) minimizing the potential for damage in the event of an attack.

The overall practical objective of the proposed security program is, therefore, not to provide full protection, but to discourage terrorist attack through visible security and reduced vulnerability, as well as to minimize damage in the event of an attack. To protect these assets, the following countermeasures are proposed as retrofits on critical bridge, interchange, and tunnel assets:

- Maximize potential explosives placement standoff distance to key structural members or mechanical systems via various types of barriers.
- Deny access to locations where placement of explosives would affect points of structural integrity and vulnerability for infiltration of mechanical systems through the installation of locks, caging, and various types of fencing.
- Minimize time-on-target for terrorists via installation of real-time intrusion detection and surveillance systems.
- Selectively protect the structural integrity of key members against collapse by strengthening key substructure members and blast shielding.

In addition, these strategies are also assumed to be routinely applied to larger bridges as they undergo their normal reconstruction cycle.

Total costs for this asset protection initiative are estimated at $2.4 billion over the six-year period, including $1.5 billion in capital costs and $880 million for operations and maintenance (O&M). These numbers breakout as follows: (1) bridges: $1.4 billion in capital costs and $880 million for O&M, (2) tunnels: $60 million in capital costs, and (3) transportation management centers: $50 million in capital costs.

Enhancing Traffic Management Capabilities

Many of the nation’s larger metropolitan areas are already installing advanced traffic management systems to better manage normal congestion. Expanding deployment of these "intelligent transportation systems" (ITS) is under discussion as a focus of current AASHTO and FHWA (Federal Highway Administration) Reauthorization concepts.

Systematic region-wide deployment of such systems could also substantially enhance the ability of metropolitan roadway systems to support terrorism-related evacuation and emergency response. Seventy-eight metropolitan areas with populations over 550,000 are identified for initial implementation. These 78 metro areas collectively encompass 10,500 miles of freeways and expressways and 16,000 miles of signalized principal arterials. In addition, 1,800 miles of connector routes on the Department of Defense
Strategic Highway Network (STRAHNET) are included in this initiative because they link to highway-dependent military installations.

The improved evacuation and emergency access capabilities are achieved by the following program:

- Deployment of ITS technologies on the applicable roadways, including (1) automatic vehicle detection, (2) camera surveillance, and (3) variable message signs – together with their integration into existing traffic management centers.

- Establishment of nine new regional security guidance centers capable of issuing real-time, event-responsive routing directives during emergencies based on remote imaging, incident tracking, and dynamic routing technologies.

Total costs for this initiative are estimated at $5.6 billion over the six-year period, including $3.7 billion in capital costs and $1.9 billion for O&M.

**Improving State DOT Emergency Response Capabilities**

The third program area is focused on upgrading the capabilities of state transportation agencies to conduct their emergency preparation, response, and recovery responsibilities as part of state and local emergency management during and after a terrorist incident.

Within existing statewide “all hazard” emergency management planning, there is an opportunity to strengthen the role of state DOTs through capitalizing on their distributed personnel, incident response training, and statewide communications networks. To achieve these objectives, the following state DOT program elements are proposed:

- Strengthen state DOT emergency operations plans and develop specific procedures for various types of terrorist incidents.

- Conduct detailed terrorist incident response training for state DOT personnel, including the staging of interagency emergency response exercises.

- Develop and deploy hardened and interoperable statewide communications networks.

- Prepare network traffic management and surveillance systems for emergency evacuation and access operations.

- Expand and upgrade real-time security operations and coordination, including protection of traffic management centers.

Total costs for this set of countermeasures are estimated at $2.5 billion over the six-year period, including $940 million in capital costs and $1.6 billion for O&M.
Total Six-Year Costs

Table 1 below presents total estimated six-year costs for the proposed AASHTO national highway security program. Capital, operating, and maintenance costs are included for the three program elements. The time phasing assumptions of this program are intended to reflect the technical and administrative feasibility of executing the improvements.
Table 1: Annual and Six-Year Total Costs Summary for Highway-Related Security Programs

<table>
<thead>
<tr>
<th>Program</th>
<th>Program Elements</th>
<th>Capital Costs (in millions)</th>
<th>Six Year Capital Costs (in millions)</th>
<th>Six-Year Operating Costs (in millions)</th>
<th>Average Annual O&amp;M Costs (in millions)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Year 1</td>
<td>Year 2</td>
<td>Year 3</td>
<td>Year 4</td>
</tr>
<tr>
<td>Protection of Critical Mobility Assets</td>
<td>Bridge retrofit</td>
<td>$245</td>
<td>$245</td>
<td>$245</td>
<td>$245</td>
</tr>
<tr>
<td></td>
<td>Bridge reconstruction</td>
<td>$70</td>
<td>$70</td>
<td>$70</td>
<td>$70</td>
</tr>
<tr>
<td></td>
<td>Tunnels</td>
<td>$30</td>
<td>$30</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Transportation management centers</td>
<td>$25</td>
<td>$25</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enhancement of Traffic Management Capabilities</td>
<td>Detection, surveillance, message signing &amp; dynamic routing</td>
<td>$609</td>
<td>$609</td>
<td>$609</td>
<td>$609</td>
</tr>
<tr>
<td>Improvement of State DOT Emergency Response</td>
<td>Planning, training, communications</td>
<td>$156</td>
<td>$156</td>
<td>$156</td>
<td>$156</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$1,080</td>
<td>$1,135</td>
<td>$1,135</td>
<td>$1,080</td>
</tr>
</tbody>
</table>
Part I. Highway-Related Security Program Overview

1. Introduction

1.1 AASHTO Reauthorization Security Policy

This report has been prepared to develop further the concepts and costs presented in the security policy component of the American Association of State Highway and Transportation Officials (AASHTO) Reauthorization proposals and dimensioned in the AASHTO 2002 Bottom Line Report.

On April 21-22, 2002, the AASHTO Board of Directors adopted a preliminary set of policy recommendations for inclusion in Reauthorization of the Transportation Equity Act for the 21st Century (TEA-21); current authorization expires on September 30, 2003. In the policy recommendations, AASHTO TEA-21 Reauthorization Policies; Topic VIII: Security/Overview reads as follows:

“The heightened threat of terrorism introduces new imperatives, of a type never faced before, to the nation’s highway and transit programs. The specter of international terrorism armed with weapons of mass destruction establishes a new context for security policy and planning. This context includes not only an expanded threat matrix (explosive, chemical, biological and radiological) but also the potential of a variety of delivery mechanisms, combinations and environmental settings.

While the surface transportation infrastructure is robust and redundant, the consequences, both direct and indirect, of a major attack can be significant. There are contexts across the United States in which the loss of key links could have significant economic and mobility consequences – not to mention immediate loss of life. Surface transportation infrastructure is important not just from the perspective of maintaining its normal important functions but also for its emergency response utility in the context of a terrorist incident on or off the transportation system, as with the September 11, 2001 events.

Therefore, government has a responsibility to minimize the vulnerability of critical transportation infrastructure assets and to prepare for transportation’s role in emergency response and recovery. While the emergency management community has the lead on many of these matters, there are key issues with significant additional resource implications that must be faced by the federal and state departments of transportation. These include: upgrading state DOT emergency operations capabilities; protection of key facility assets; and improving emergency traffic management capacity. Some of these issues can be addressed through TEA-21 authorization.”
1.2 Focus of this Report

The focus of this report is twofold. First, it is designed to assist AASHTO in refining the security cost component of its Bottom Line Report by providing an estimate of highway security needs in terms of six-year capital and operating costs related to Reauthorization of the Federal Aid Highway Program.

Secondly, the report also provides the basis for further consideration of key policy, programmatic, and research issues in areas critical to emergency management planning. This report outlines key state department of transportation (DOT) responsibilities in the cycle of mitigation/preparedness/response/recovery. Three major program areas included in the proposed AASHTO security program address these responsibilities:

- **Protection of Critical Mobility Assets**: Key bridges, tunnels, and interchange structures essential to the function of the highway network at the interregional and national scale and, therefore, deserving of protective countermeasures.

- **Enhancement of Traffic Management Capabilities**: Metropolitan roadway facilities selected for enhancement for evacuation and monitoring capabilities for both terrorism and other emergency purposes.

- **Improvement of State DOT Emergency Response**: State DOT emergency response capabilities that require improvement to meet security needs.

The conduct of the work has followed a common process for each of the three areas, including the following steps:

- Establish potential threat dimensions and identify those considered reasonable for deterrence/defense and/or response.

- Develop definition of critical assets and key emergency response activities.

- Establish generic asset vulnerabilities and appropriate countermeasures.

- Estimate six-year capital and operating costs.

1.3 Focus on Terrorism and Weapons of Mass Destruction (WMD)

Transportation assets take on special significance in a terrorist-related context. Terrorist objectives are presumed to be political, economic, and social disruption via damage and destruction of physical facilities, civilian deaths and injuries, and public demoralization. These objectives are leveraged by the will to use weapons of mass destruction (WMD). These weapons are, by definition, those that can destroy large numbers of people and include high explosives, nuclear, biological, chemical, and...
radiological devices and other unconventional means of delivering large destructive force.

WMD introduce a focus on the potential of highway facilities as both target and response. Despite the robust and redundant nature of the highway system, the use of such weapons has greater potential for destroying and disrupting critical links of the highway network than lesser weapons – and could substantially disrupt important economic and mobility functions. While such facilities may not be the most attractive targets, the potential for attack and major consequences cannot be discounted, and appropriate measures must be considered.

At the same time, the highway also plays a key role in emergency response to any type of major terrorism incident – by supporting state and local emergency management activities and through the potential to provide emergency access and evacuation capacity. Each of these dimensions relates to a key security program initiative discussed in this report.

While terrorism is not new, the power of terrorist weapons and/or the capability to deliver those weapons has rapidly expanded in the last half-century. Terrorists now have demonstrated improvised weapons with massive destructive capabilities. Two key dimensions of terrorist incidents distinguish them from the conventional disasters with which state emergency management and state DOTs routinely cope. The first is the characteristics and effects of the weapons. Table 2 below indicates the range of different effects on people and property, highlighting some of the key consequences of several types of WMD that might be considered threats to infrastructure:

**Table 2: WMD Characteristics and Effects on Infrastructure and Other Targets**

<table>
<thead>
<tr>
<th>WMD</th>
<th>Possible Distinguishing Signs</th>
</tr>
</thead>
</table>
| **Conventional Explosives** (e.g., detonation of military-type or commercial bombs, such as fuel oil-fertilizer, etc.) | • Explosions  
• Casualties  
• Various types of localized blast damage up to structural collapse  
• Exposure to dust and hazardous building materials, e.g., asbestos  
• May be used to spread harmful radiological or chemical materials |
| **Chemical** (e.g., dispersion of pesticides, mustard gas, chlorine gas, cyanide, tear gas, etc.) | • Initial unexplained deaths and illnesses  
• Effects mostly localized to release site, but may be distributed beyond release site by wind and contamination  
• Area may be marked by unusual clouds, haze, mist, odors, tastes, droplets, etc.  
• May be persistent in environment |
| **Biological** (e.g., dispersion of viruses, bacteria, toxins, fungus, etc.) | • Initial unexplained deaths and illnesses, possibly beginning a day or more after an incident |
The second difference is that terrorist WMD attacks have special characteristics that affect the nature of the appropriate preparedness strategies and response actions. These differentiate them from natural disasters. Table 3 below suggests the key similarities and differences between, for example, a typical hurricane and a terrorist attack.

### Table 3: Possible Similarities and Dissimilarities between Terrorist WMD and Natural Disasters

<table>
<thead>
<tr>
<th>Similarities</th>
<th>Dissimilarities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mass casualties</td>
<td>Caused by people on purpose</td>
</tr>
<tr>
<td>Damage to infrastructure</td>
<td>May target specific security vulnerabilities</td>
</tr>
<tr>
<td>Occurs with or without warning</td>
<td>Affected areas will be treated as crime scenes</td>
</tr>
<tr>
<td>Evacuation or displacement of citizens</td>
<td>May not be immediately recognizable as terrorist events</td>
</tr>
<tr>
<td></td>
<td>May not be single events</td>
</tr>
<tr>
<td></td>
<td>Place responders at higher risk</td>
</tr>
<tr>
<td></td>
<td>May result in widespread contamination of critical equipment and facilities</td>
</tr>
<tr>
<td></td>
<td>May expand geometrically in scope</td>
</tr>
<tr>
<td></td>
<td>May cause strong public reaction</td>
</tr>
</tbody>
</table>
Key assumptions that may be drawn from the nature of the terrorist threat underlying the strategies described and costed in the report include:

- **Terrorist objectives are presumed to be political, economic and social disruption via damage and destruction of physical facilities, civilian deaths and injuries, and public demoralization via disruption resulting from responses to credible threats.**

- **State DOTs are a key support component of overall statewide and local emergency response programs. Highway systems provide a critical emergency response mechanism to off-road incidents and can be equipped to improve the efficiency of that role.**

- **Transportation assets in general have relatively low attractiveness as terrorist targets because of the modest potential for casualties. Regarding highway infrastructure, terrorism objectives are therefore likely to focus on destruction/damage to the physical assets rather than on the transient use population. They also tend to focus on targets with high symbolic value.**

- **Some highway structures, for example, major bridges and tunnels, play essential connecting roles and serve unique transportation and economic roles, and should therefore be considered for protection in order to maintain their functionality.**

2. **Development of the Program Estimates**

2.1 **AASHTO Security Programs**

AASHTO’s Reauthorization proposal includes a significant security component with major resource implications. The security proposals were developed in concept by the AASHTO Reauthorization Task Force and reflect the focus of the AASHTO Transportation Security Task Force interests, including vulnerability assessment and the emergency response guides developed through NCHRP for the Task Force. The proposals were adopted by the AASHTO Board of Directors.

This Report provides the background for the three major security components of the AASHTO Reauthorization proposal:

- **An asset protection/countermeasures program for critical highway-related assets.**

- **An initiative to extend and upgrade traffic management systems in major urban areas for emergency routing for evacuation and emergency access.**

- **Improvements in the state DOT emergency response and operations capabilities and facilities.**
The three programs are developed at a high level of generality for the purposes of making reasonable cost estimates on a national basis covering the potential activities of all AASHTO member departments. Given the absence of publicly available national security policy regarding highway transportation assets, preparation of these estimates requires making a range of assumptions about general policy, program activities, and coverage. These assumptions are built on the previous security studies by AASHTO, preliminary concepts under discussion in the state emergency management community, Federal Highway Administration (FHWA) documentation, discussions with both governmental and non-governmental technical experts, and open-source material in the security area.

For each of the three programs, the key threats and vulnerabilities are characterized, potential consequences reviewed, and critical assets identified. The proposed security programs are then hypothetically scoped for state DOTs with due regard for typical existing capacities. The program scopes are used as the basis for order-of-magnitude estimates of capital and operating costs. These estimates are predicated either (1) on the appropriate national asset “system” involved (i.e., the critical asset protection and enhancement of traffic management programs), or (2) at the level of an “average” state DOT and then scaled up to a national basis (i.e., for the program for improving emergency response capabilities). Estimates are provided for capital and operating costs for the six-year Reauthorization period.

2.1.1 Caveats and Uncertainties

This work was conducted within a context with considerable uncertainties:

- Regarding highway-related assets, there is currently no accepted national doctrine regarding terrorist threat capabilities and threat characteristics beyond the Office of Homeland Security (OHS) threat warning levels and related Transportation Security Administration (TSA) threat level response criteria.

- There are no accepted or other open-source criteria established by federal security or transportation agencies for definitions of critical highway assets or for appropriate security programs.

- Emergency response program experience is built largely from natural disasters and the special circumstances surrounding the attacks of 9/11. There is no broad acceptance of the appropriate level for investment in emergency preparedness.

- Many of the technical issues relating to the interactions between WMD blast phenomenology and transportation infrastructure, as well as appropriate countermeasure design, are not addressed in open-source material. In addition, many key countermeasure issues relating to highway structures are in the early stages of research.
Therefore, in light of the above uncertainties, the authors of this report have made assumptions based on available source materials, limited technical analysis, and expert opinion.

In the material below, brief summaries of each of the three programs are presented.

2.1.2 Program for Protection of Critical Mobility Assets

There is a range of important transportation system assets that are potentially vulnerable, including elements of the aviation, transit, and intermodal freight system, that are already receiving considerable national attention. Within highway transportation, there are also important assets, such as key bridges, tunnels, and interchange structures, essential to the functioning of the highway network at the interregional and national scale and therefore deserving of protective countermeasures.

As owner-operators of such facilities, state and local transportation departments and authorities must consider the relative threats to highway structures and identify those facilities that may be deemed “critical” as priority candidates for appropriate protection against terrorist threats, especially explosive attacks. Preliminary guidance for this activity was presented in AASHTO’s Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection (NCHRP Project 20-7).

For purposes of developing an aggregate national level cost estimate, this study established a set of criteria to identify “critical” facilities including:

- Role in interregional economy (e.g., size, network role, redundancy).
- Replacement cost and down time.
- Visibility as regional and national symbols (e.g., Golden Gate Bridge).

Using the existing highway, bridge, and tunnel databases and the management systems of the FHWA and states, it was determined that approximately 450 existing bridges and 50 tunnels meet criteria thresholds based on facility size and traffic volumes, and on their role in the Interstate System and the Strategic Highway Network (STRAHNET). A small portion of these critical assets was also assumed to possess special symbolic attraction to terrorists and was therefore accorded an extra level of protection.

The facilities classified as “critical” cover a wide range of bridge and tunnel structure types with a variety of settings, ages, and vulnerabilities. At the same time, the range of weapon size and attack mode options may vary broadly from “backpack” bombs to large truckloads of high explosives. Current military and engineering judgment indicates that complete protection from destruction of key structural elements is not feasible or cost-effective. The overall practical objective of various security measures is, therefore, not to provide full protection, but to discourage terrorist attack through visible security and reduced vulnerability, as well as to minimize damage to such facilities in the event of an attack. An effective security program thus not only protects critical assets, but may
induce terrorists to focus on less critical assets by increasing the risks of terrorists’ capture, as well as the costs, complexity, or risks of an attack. A layered approach has been adopted incorporating the “4-Ds” of counter-terrorism: Deterrence, Detection, Defense, and Design.

The countermeasure program, therefore, includes elements with the following objectives:

- **Maximize explosive standoff distance** to key structural members or mechanical systems via various types of barriers, including pier and abutment fencing and pier dolphins.

- **Deny access** to locations where placement of explosives would affect points of structural integrity and locations of vulnerability for infiltration of mechanical systems through the installation of locks, caging, and various types of fencing.

- **Minimize time-on-target** for terrorists to undertake strategically placed or coordinated detonations via installation of real-time intrusion detection and surveillance systems connected to transportation management centers, backed by security patrol response.

- **Selectively protect** the structural integrity of key members against collapse by strengthening key substructure members and blast shielding.

Generic countermeasures were defined for three major bridge types and for major tunnels. Unit costs were applied to the aggregate critical inventory to determine total capital and operating and maintenance costs. These costs were spread over the Reauthorization period as appropriate. In addition, costs were added to account for the marginal expense of applying new security design criteria to new bridges and tunnels and for major reconstruction projects. The background for these estimates is presented below in Part II, Section 3, Program for Protection of Critical Mobility Assets. The generic strategies and costs are shown, respectively below, in Table 4, National Highway-Related Security Program Cost Structure, and Table 5, Annual and Six-Year Total Costs Summary for Highway-Related Security Programs.

### 2.1.3 Program for Enhancement of Traffic Management Capabilities

The second element of the proposed overall security program is a program that capitalizes on the potential of the metropolitan roadway systems to protect and support threatened populations. This is accomplished by improving the capabilities of the urban roadway system to support terrorism-related evacuation and emergency response. In concept, this program parallels the congestion-related operational needs as identified in other current AASHTO and FHWA programs and Reauthorization concepts under discussion.
Approximately 25 percent of the freeway network in the 78 largest metropolitan areas of the United States has already received traffic monitoring and surveillance systems deployment. The hypothesized program would upgrade the remaining major network components in the largest metropolitan areas, providing the ability to monitor traffic conditions, view major incidents, and communicate with users in the event of major incidents or emergencies.

The major criteria for facility inclusion in the program are network role and traffic volume. This network incorporates about 10,500 miles of freeway and expressway and approximately 16,000 miles of principal arterials with a current volume/capacity ratio of over 0.5 in the 78 metropolitan areas. An additional 1,800 route miles is included to reflect nine STRAHNET “fort-to-port” connector routes supporting the most highway-dependent military installations.

It is assumed that this network will receive the installation of systems to enhance its capabilities for emergency management including bypass, access, and evacuation functions. The systems include:

- Automated vehicle detection technology to track system use, performance, and incidents.
- Surveillance systems, e.g., CCTV (closed-circuit television), to observe incidents and other problems from DOT operations and emergency management centers.
- Variable message signs on principal routes to guide users regarding evacuation, emergency procedures, and routes.

In addition to equipping the facilities and integrating the new systems into upgraded traffic management centers, an additional strategic program assumes establishment of federal/state-run security guidance centers. These centers are assumed to be capable of applying new remote imaging technology, incident dynamics, and real-time routing systems. Such capabilities could provide event-responsive dynamic routing directives in real-time with the appropriate regional and interregional integration.

System unit costs are applied to the assumed network to determine total capital and maintenance costs. These costs are spread over the Reauthorization period as appropriate. In addition, costs are added for annual operations and maintenance. The background for these estimates is presented below in Part II, Section 4, Program for Enhancement of Traffic Management Capabilities. The generic strategies and costs are shown, respectively below, in Table 4, National Highway-Related Security Program Cost Structure, and Table 5, Annual and Six-Year Total Costs Summary for Highway-Related Security Programs.

2.1.4 Program for Improvement of State DOT Emergency Response

State DOTs provide support functions in the existing emergency response plans of state emergency management agencies. These “all-hazard” statewide plans have proven to
be robust tools for natural disasters. However, the 9/11 experience has indicated the need to update and modify these statewide plans, including the supporting emergency operations plans of the state DOTs. Key challenges that are the focus of such efforts include:

- Absence of interoperable and reliable communications among agencies.
- Lack of familiarity with the roles and personnel of other agencies.
- Responding to the introduction of Federal law enforcement and security agencies.
- Handling terrorist incident venues as crime scenes.
- Unfamiliarity with Incident Command System practices of public safety agencies.
- Protection of first responders from biological, chemical, and radiological hazards.
- Need for specific traffic operations regimes, such as evacuation and emergency access and the untapped potential of Intelligent Transportation Systems technology for control and communications.
- The lack of national training standards for first responders in dealing with acts of domestic terrorism.

Many state DOTs are working closely with their state emergency management agencies to better adapt the statewide plans to the challenges of terrorism and are currently in the process of updating their emergency operations plans. Some of these activities indicate an increased role for transportation to capitalize on DOTs distributed personnel, incident response training and statewide communications networks. Furthermore, state DOTs are increasing their capacity to monitor and view highway conditions as well as apply management and communications facilities to support emergency movement of people and goods during and after an incident.

Activity costs were developed on a state basis assuming application to the “average” state DOT. The specific assumptions about the program elements and their costs are based on the precursor AASHTO Guide to Updating Highway Emergency Response Plans for Terrorist Incidents (NCHRP Project 20-7/151A), as well as recent discussions with active states. The program elements include:

- General emergency management planning, training, and exercises including interagency activities.
- Planning for key security elements including vulnerability assessment, hazard mitigation, and evacuation systems planning.
• Development and deployment of expanded interoperable interagency communications.

• Expanded and upgraded real-time security operations and coordination including the protection of traffic management centers.

Many of the costs involved in improved emergency management are operating costs, rather than capital in nature. These costs were spread over the Reauthorization period as appropriate. The background for these estimates is presented in Part II, Section 5, Program for Improvement of State DOT Emergency Response. The generic strategies and costs are shown, respectively below, in Table 4, National Highway-Related Security Program Cost Structure, and Table 5, Annual and Six-Year Total Costs Summary for Highway-Related Security Programs.

2.2 Dual Use Benefits

The proposed investment program, described above, is designed to meet essential national security needs. However, the program has also been developed to capitalize on dual use benefits such that its policy rationale and cost-effectiveness are substantially enhanced. Examples of these dual payoffs include:

• Security countermeasures for bridges over navigable waterways, e.g., lighting, pier strengthening, and pier dolphins, will contribute to overall bridge safety.

• Tunnel security improvements are assumed to simultaneously meet NFPA (National Fire Protection Association) 502 life-saving standards, e.g., detection and surveillance, enhanced communications, and fire lines.

• Highway emergency management systems for evacuation and emergency access – including detection, surveillance, and traveler information applications – are needed to improve the operational efficiency of congested metropolitan areas, as well as to serve natural and non-terrorist technological disaster evacuation purposes.

• Improved terrorism-responsive emergency management facilities and procedures, such as integrated and interoperable interagency communications, provide the basis for augmented incident and non-terrorism-related emergency management.

These non-security benefits substantially enhance the justification for the proposed security investment level.

2.3 Total Security Investment Needs

Table 4 below summarizes the program focus of the cost estimates.
Table 4: National Highway-Related Security Program Cost Structure

<table>
<thead>
<tr>
<th>Program</th>
<th>Assets</th>
<th>Coverage</th>
<th>Capital Costs</th>
<th>Operations &amp; Maintenance Costs</th>
<th>Dual Use</th>
</tr>
</thead>
</table>
| Protection of Critical Mobility Assets | • Critical bridges  
• Critical tunnels  
• Transportation management centers (TMCs) | • Critical facilities with national economic, defense & emergency route importance | • Non-structural counter-measures  
• Limited structural mitigation | • Systems maintenance                                                                 | • Safety                 |
| Enhancement of Traffic Management Capabilities | • Major metropolitan freeway & arterial networks | • Top 78 metro areas | • Surveillance & detection systems  
• Traveler information systems | • Systems maintenance                                                                 | • Urban mobility       |
| Improvement of State DOT Emergency Response | • State DOT capabilities & systems  
•all state DOTs | • All state DOTs | • Communication system upgrades | • Staffing  
• Planning  
• Training  
• Exercising  
• Security systems support | • Incident and emergency management                                       |

Table 5 below provides a summary of the six-year Reauthorization cost estimates for capital investments as well as certain related operations and maintenance for the three program elements. The time phasing assumptions of this program are intended to reflect the technical and administrative feasibility of executing the improvements:

- It is assumed that implementation of non-structural protective measures to bridges and tunnels are to be executed within two years given the need to move quickly to secure critical assets, while structural modifications are assumed to take approximately four years.

- Average annual facility-related annual operating and maintenance costs are shown over the six-year period and are based on the cost of installed capital facilities requiring operations and maintenance.

- Emergency response program costs (non-capital) are shown annually.

In the sections that follow, each of the programs is discussed in greater detail, including threat assumptions, response strategy, program elements, and costs.
## Table 5: Annual and Six-Year Total Costs Summary for Highway-Related Security Programs

<table>
<thead>
<tr>
<th>Program</th>
<th>Program Elements</th>
<th>Capital Costs (in millions)</th>
<th>Six Year Capital Costs (in millions)</th>
<th>Six-Year Operating Costs (in millions)</th>
<th>Average Annual O&amp;M Costs (in millions)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection of Critical Mobility Assets</td>
<td>Retrofit bridges</td>
<td>$245 $245 $245 $245</td>
<td>$980</td>
<td>$660</td>
<td>$110 per year</td>
</tr>
<tr>
<td></td>
<td>Bridge reconstruction</td>
<td>$70 $70 $70 $70 $70</td>
<td>$420</td>
<td>$222</td>
<td>$37 per year</td>
</tr>
<tr>
<td></td>
<td>Tunnels</td>
<td>$30 $30</td>
<td>$60</td>
<td>Costs not attributable directly to security</td>
<td>Costs not attributable directly to security</td>
</tr>
<tr>
<td></td>
<td>Transportation management centers</td>
<td>$25 $25</td>
<td>$50</td>
<td>Costs not attributable directly to security</td>
<td>Costs not attributable directly to security</td>
</tr>
<tr>
<td>Enhancement of Traffic Management Capabilities</td>
<td>Detection, surveillance, message signing &amp; dynamic routing</td>
<td>$609 $609 $609 $609 $609 $609</td>
<td>$3,654</td>
<td>$1,914</td>
<td>$319 per year</td>
</tr>
<tr>
<td>Improvement of State DOT Emergency Response</td>
<td>Planning, training, communications</td>
<td>$156 $156 $156 $156 $156 $156</td>
<td>$936</td>
<td>$1,638</td>
<td>$273 per year</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td>$1,080 $1,135 $1,135 $1,080 $835 $835</td>
<td>$6,100</td>
<td>$4,434</td>
<td>$739 per year</td>
</tr>
</tbody>
</table>
Part II. Security Programs

3. Program for Protection of Critical Mobility Assets

3.1 Risk Management Strategy

The development of this program was based on a systematic risk assessment approach at the appropriate level for determining national aggregate costs.

Key threats were identified in terms of targets of attraction and potential methods of attack. Critical assets within the highway system were identified based on assumed national level criteria regarding the potential consequences of damage or destruction. The risks to key asset classes were then assessed, responding principally to the generic vulnerabilities of each asset class. Deterrent and mitigation countermeasures were specified and costed using current unit costs. Most of the proposed measures are modest retrofits designed for deterrence and detection with minimal hardening investments.

A countermeasure program must make reasonable assumptions about the nature of threats faced in order to determine an appropriate countermeasures strategy. The definition of the programs assumed for these security programs was built on a series of risk management assumptions: (1) that any particular terrorist target event is essentially a low probability, high consequence event, and as such, risk mitigation strategies should differentiate among priorities, based on target criticality; and (2) that reasonable risk for critical assets must be accepted since mitigation is necessarily incomplete.

3.2 Threat Assumptions

Terrorists have a history of attacking transportation assets such as cars and buses. These attacks have normally been associated with violent explosions and/or gunfire. However, the face of terrorism has been changing over the years. Today’s international terrorists have been moving from isolated bombings, hijackings, and hostage-taking to the indiscriminate slaughter of innocent men, women, and children. The recent terrorist trend is toward inflicting a high number of civilian casualties, more extensive property damage, and the increasingly devastating effects on economies. Last year’s World Trade Center attack, the Atlanta Olympics and Oklahoma City bombings, and the gassing of the Tokyo subway a few years ago killing 10 and injuring over 5,000, evidence this shift.

However, compared to other transportation modes, physical highway assets are relatively robust and redundant, and the mass casualty potential is lower than other types of targets. Nonetheless, the use of large WMD has greater potential of destroying and disrupting critical transportation and economic links of the highway network than lesser weapons. At the same time, components of the highway system can play an essential emergency management function. Therefore, while it is appropriate that other
assets may receive priority attention for their mass casualty vulnerability, responsible owner-operators should consider the protection of key assets from the point of view of the consequences of loss by direct attack as well as in the context of attacks on other assets.

Key assumptions underlying the threat assessment include:

- **Terrorist objectives are presumed to be political, economic, and social disruption inflicted through damage and destruction of physical facilities, large numbers of civilian deaths and injuries, and public demoralization.**

- **The preferred targets for terrorist attacks continue to be "soft" targets, such as business, tourist sites, and facilities with limited security precautions.**

Transportation assets generally have relatively low attractiveness as terrorist targets because the potential for casualties is fairly modest. Transit and rail systems are regarded by law enforcement to be more likely targets. Highway assets in particular seem less attractive as targets, given their physical robustness, systems redundancy, and relative ease of replacement.

- **However, some highway structures, like major bridges and tunnels, play critical roles spanning large natural barriers such as rivers, bays, mountains, and serve unique regional and national transportation and economic roles. Major damage or destruction of these structures could have severe economic and mobility consequences.**

- **Regarding highway infrastructure, terrorism objectives may focus on destruction/damage to the physical assets as well as the transient use population.**

- **Open source material indicates that Al-Qaeda-type terrorists also appear to be attracted to targets with high symbolic value. Some bridges and tunnels have high visibility and constitute regional and national symbols.**

- **Terrorist tactics seem to focus on attacks that are relatively simple, easy to coordinate, and utilize readily available materials, relying on secrecy, surprise, and speed.**

- **Of those assets under state DOT jurisdiction, major bridges (including interchange bridges) and tunnels are generally assumed to be the most attractive terrorist targets. Headquarters, district, and maintenance facilities appear to be less threatened as probable targets of a terrorist attack; however, disruption of operations in such facilities could significantly impair delivery of public services.**

Terrorist threats theoretically include the complete array of WMD – conventional explosives, chemical, biological, and nuclear/radiological weapons. However, bridges and tunnels are not likely to be prime targets for WMD of the chemical, biological, or
radiological variety that would normally target civilian population concentrations. This is not to say that a radiological or biochemical attack against a bridge or tunnel is not possible; rather that it is a less probable threat. Limited physical, on-site countermeasures related to bridge and tunnel design or operations with respect to chemical, biological, or radiological threats are included. These are focused on the tunnel ventilation systems. More general deterrence against such WMD attacks with their presumed population targeting is appropriately part of security and law enforcement jurisdiction – not public works entities.

Open-source literature indicates that Al-Qaeda-type terrorist attacks seem to be characterized by “high concept/low tech” approaches with a preference for explosive force and martyr risks. Therefore, this analysis focuses on explosive attacks including as threats a range of such weapons as:

- Portable, hand-placed cutting charges placed on or near structures, e.g., 100 pounds of C4;
- Vehicle or boat-borne explosives, e.g., the 4,000 pounds of explosives of fertilizer/oil mix (ANFO) used in the Murrah Center attack; and
- Up to 60,000 pounds of explosives delivered in semi-trailers or boats of various sizes.

These weapons may be maneuvered to locations immediately adjacent to, under, or even inside structures. Remote rocket and missile-borne explosive attacks are theoretically possible, but not likely, and countermeasures within a state DOT’s jurisdiction are limited. Figure 1 below from the Federal Alcohol, Tobacco and Firearms (ATF) Agency website illustrates the range of most likely options and their impacts on people.
Terrorist threats to transportation facilities may include:

- Structural/functional damage/destruction resulting from portable, truck-or boat-borne explosives and fire damage.

- Casualties from blast or fire.

- System shutdown via exposure and contamination from biological and/or chemical WMD, e.g., introduced through tunnel vents.

- Collateral damage to other lifelines, e.g., telecommunications, power, and pipelines carried along bridges or tunnels.

Vulnerabilities and countermeasures discussed below are defined with reference to these types of threats.

### 3.3 Definition of “Critical” Highway System Assets

The Nation’s highway infrastructure is robust. Compared to other transportation assets, the highway infrastructure is relatively invulnerable. Highways and associated facilities are part of networks with a high degree of ubiquity and redundancy. Loss of individual
assets could, in some cases, be substantially inconvenient and damage a local economy, but the damage would not be permanent or irreparable. In addition, the physical structures are, by design, relatively resistant to major forces. In some cases, structures are designed to absorb accidents through the use of pier ramming design criteria. It makes sense, therefore, to concentrate protective measures on the segment of the asset inventory where destruction would have the greatest consequences.

Critical Assets and Recognizable Assets

Not all assets are equally important in their function. As a point-of-departure risk management assumption, the most “critical” assets – from a national perspective – are identified from a consequence perspective; that is, critical assets are those major facilities the loss of which would significantly reduce interregional mobility over an extended period and thereby damage the national economy and defense mobility. Such assets include major bridges (including key urban interchange components) and major tunnels on the upper-level highway system in the U.S. that play significant roles in linking important economic activity centers, markets and production centers, urban centers and suburbs, military forts, and ports – across major physical boundaries such as rivers, mountain chains, estuaries, and bays. These may appropriately be classified as “critical”.

The risk management perspective applied also presumes that even among the most consequence-based “critical” assets, certain assets may be more likely targets, based on the type of thinking that characterizes international terrorists, such as Al-Qaeda. These assets are those that are “recognizable” – highly visible and well-known symbols of a nation or region, the loss of which could demoralize the public as well as be costly or greatly inconvenient. These structures or facilities should be singled out for extra security precautions.

In addition, there are agency assets, such as transportation management centers, the loss of which would significantly handicap emergency response functions. These types of activities are often housed in unprotected commercial buildings. These are also classified as “critical” for the purpose of this analysis.

Critical Bridges

There are over 582,000 bridges in the U.S. over 20 feet in length. As there are no open-source “official” criteria or lists of critical assets, state and authority transportation systems owner-operators will have to make their own determinations as to which structures or facilities to protect and the appropriate level of protection. AASHTO has produced guidance material, and several states are conducting systematic vulnerability analyses and assessing appropriate protective measures.

For purposes of making a national aggregate estimate of security costs, a definition of “critical” bridges and tunnels was developed. A broad set of criteria reflecting national significance was applied, utilizing the comprehensive 165-item database of bridge
characteristics in the FHWA National Bridge Inventory (NBI). Critical bridges were defined by functional criteria and presumed to be those deserving of a basic level of protective actions.

The criteria employed to define nationally “critical” include:

- **Casualty Risk – Number of users exposed as reflected in:**
  - The main span size of the bridge, that is, over 50m/165 feet, and
  - Traffic over 40,000 average daily traffic (ADT).

- **Economic Disruption – Disruption of the national economy as indicated by:**
  - Bridges located on the Interstate Highway System plus the Department of Defense-defined Strategic Highway Network (STRAHNET),
  - Traffic over 40,000 ADT,
  - Main span length over 50 meters/165 feet,
  - Double deck bridges, and
  - Nearest detour distance more than 5 km/3 miles for bridges under 60,000 ADT.

- **Military Support Function:**
  - Bridges on STRAHNET and/or on the Military Traffic Management Command (MTMC)-defined “Power Projection Routes” serving forts within 400 miles of port, and
  - Main span over 50m/165 feet.

- **Emergency Relief Function:**
  - Bridges in 78 major metropolitan areas, and
  - On upper level system, i.e., freeways, expressways, and principal arterials.

- **National Recognition:**
  - Bridges with symbolic importance.

- **Collateral Damage Exposure:**
  - Bridges carrying other utilities, e.g., pipelines and major power and communications lines.

Application of these criteria results in a group of 391 bridges on the 45,376-mile Interstate System and an additional 60 bridges on the 15,668 miles of STRAHNET. This list of 451 includes most of the larger bridges that span the Mississippi and other larger rivers, and major estuaries on all coasts. 142 of the “critical” bridges cross navigable waterways such as major rivers, harbors, and estuaries. The list also includes components of major urban interchanges, i.e., 166 bridges have additional highway service underneath.

Table 6 below indicates the approach to the definition of “critical” for bridges:
### Table 6: Determination of "Critical" Bridges

<table>
<thead>
<tr>
<th>Criticality Factor</th>
<th>Function of:</th>
<th>Proxy</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Casualty Risk</td>
<td>Users exposed</td>
<td>Main span length &gt; 50m/165ft</td>
<td>NBI</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ADT &gt; 40K</td>
<td>NBI</td>
</tr>
<tr>
<td>Economic Disruption</td>
<td>Role in national economy</td>
<td>ADT &gt; 40K</td>
<td>NBI</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Functional system: Interstate plus STRAHNET</td>
<td>NBI</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Navigation preservation</td>
<td>NBI</td>
</tr>
<tr>
<td></td>
<td>Replacement/down time</td>
<td>Main span length &gt; 50m/165ft and structure types</td>
<td>NBI</td>
</tr>
<tr>
<td></td>
<td>Replacement cost</td>
<td>Main span length</td>
<td>NBI</td>
</tr>
<tr>
<td></td>
<td>Redundancy</td>
<td>Detour distance &gt; 5km/3mi for ADT &lt; 60K</td>
<td>NBI</td>
</tr>
<tr>
<td>Military Function</td>
<td>Support power projection platform</td>
<td>On STRAHNET and/or on MTMC “Power Projection Routes” serving forts &lt; 400 miles from ports with main span &gt; 50m/165ft; no ADT limits</td>
<td>MTMC</td>
</tr>
<tr>
<td>Emergency Relief</td>
<td>Major evacuation routes</td>
<td>Metro size (top 78)</td>
<td>FHWA</td>
</tr>
<tr>
<td>Function</td>
<td></td>
<td>Functional System: Freeways, expressways and principal arterials</td>
<td>FHWA</td>
</tr>
<tr>
<td>National Recognition</td>
<td>Symbolic importance</td>
<td>5 percent of critical bridges</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>Other</td>
<td>Collateral exposure</td>
<td>Roads on dams, pipelines, etc.</td>
<td>Not Applicable</td>
</tr>
</tbody>
</table>

#### Critical and Recognizable Bridges

It may be reasonably assumed that the critical list of 451 bridges identified by the criteria above would include most of the structures that are nationally known by proper name with specific historic or symbolic importance. For purposes of this study, five percent were assumed to be "recognizable as well as critical" and are singled out for special countermeasures as described in Section 3.5 below. It may be reasonably assumed that these are also the largest structures and carry the most traffic. Note, however, that this study is meant to be at the aggregate national level and therefore purposely does not identify the “critical” or “recognizable” assets by name or location.
Critical Tunnels

The “critical” tunnel list was developed based on material in the FHWA report, Development of a Tunnel Management System (TMS) – Phase I Report. This report is not yet complete, but it contains the only listing of most of the major tunnels. The TMS report provides limited physical and jurisdictional characteristics, e.g., size, length, and type, although, unlike the National Bridge Inventory, it does not address use intensity, detour length, or other potentially important factors. Absent additional data, the 54 tunnel facilities over 500m/1640 feet in length were identified as “critical” in light of the physical barriers to quick reconstruction and the detour implications. Eighteen of these facilities are on the Interstate Highway System. Most of these longer tunnels have updated ventilation systems and are also likely to be both staffed and equipped with up-to-date fire, incident detection, and safety equipment consistent with National Fire Protection Association (NFPA) 502 standards.

Tunnel ventilation systems represent a point of vulnerability regarding insertion of chemical and/or biological agents targeting tunnel users. While the low density of people at any given time and rate of mechanical and vehicle-induced ventilation reduces potential impacts, some protection of ventilation intakes (often associated with portal buildings) is included.

Among the 54 tunnels, 20 percent were assumed to be critical and recognizable and are singled out for special countermeasures as described in Section 3.5 below. It may be reasonably assumed that these are also the largest structures and carry the most traffic. However, it should be noted that this study is not designed for disaggregating below the national level and purposely does not identify the “critical” or “recognizable” assets by name or location.

3.4 Bridge and Tunnel Vulnerability

Protective measures discussed herein are limited to explosive attacks across the complete range of weapon size delivered as proximity attacks via mechanisms ranging from backpack to semi-trailer truck or boat.

The effect of a blast on a structure depends on several factors:

- The composition, size and shape of the explosive material (the effect of fragments from a vehicle bomb are less damaging than cased military munitions).
- The distance of the explosive from the structure (stand-off distance).
- The material composition and arrangements of the exposed structural element.

Bridges vary widely in their vulnerability depending on structure size, type, design, and setting. In general, explosives in portable quantity applied to the substructure of larger bridges are not considered a serious collapse threat – unless a terrorist demolition
expert has the time to carefully place those explosives. However, truck- and boat-borne explosives can cause more damage, including total collapse, depending on proximity, placement, and explosive yield. Table 7 below generally characterizes the possible attack scenarios considered.

Table 7: Explosive Attack Scenarios

<table>
<thead>
<tr>
<th>Mode of Attack</th>
<th>Piggy Back (hand placement)</th>
<th>Vehicle/Boat-Borne (some standoff)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scale of Charge</td>
<td>Up to 100 lbs. (TNT) per attacker</td>
<td>500 – 50,000 lbs. (TNT)</td>
</tr>
<tr>
<td>Location of Charge</td>
<td>Placed in/on pier</td>
<td>Placed on deck</td>
</tr>
<tr>
<td></td>
<td>Placed on deck</td>
<td>Placed on structural element</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Potential Form of Damage</td>
<td>Pier breach</td>
<td>Deck cratering</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The primary destructive mechanism on structures resulting from a blast is the shockwave that strikes structural members. This is a complex phenomenon responding to the geometry and composition of the structure, the angle of the blast wave, relative distances, and other factors. The resulting overpressure expands in a shock wave that is reflected by various structural elements, thereby creating a complex mix of overpressures and reflected pressures – especially in confined areas – with resulting intense and uneven impacts on the structural elements. The effects on structural members vary by type and material. On concrete members, usually not designed for load reversals and lacking ductility, they include shear cracks and compression crushing from bending on concrete members, leading to failure. On steel members, the typical failures include shear and flexure or the failure at connections and other vulnerable locations. Different structure types interact in different ways with the same blast size, and different blast sizes also exhibit non-linear characteristics depending on a number of complex interactions of blast size, shape, placement, and structural characteristics. Thus, there is large variability of expected damage by blast-structure configuration.

On a bridge structure, these types of failures may cause significant damage and can lead to progressive and systematic collapse. Countermeasures, therefore, focus on minimizing the potential for large explosives at short distances (blast yield/proximity), access to critical locations, and time on target, as well as hardening vulnerable structural elements.

For purposes of estimating countermeasure costs, bridges in the critical class were categorized by three vulnerability-based structure types since proposed countermeasures respond to vulnerability differences. Based on NBI data, the critical bridges include 19 suspension or cable-stayed bridges, 48 through-truss or arch...
bridges, and 384 “other” types, mostly girder and beam. Forty-four of the longer bridges (over 200m/650 feet total span) have significant above-deck structural components. These bridges present a more direct vulnerability to road-based attacks, just as bridges over navigable water present additional vulnerabilities to attacks on in-water piers.

There is limited open-source material discussing highway facility vulnerability other than that utilized within the Department of Defense (DOD) context. Seismic design experience has some relevance – especially regarding connections that preserve full structural capacity. Current general assumptions regarding bridge vulnerability, based on judgments by USACE (U.S. Army Corps of Engineers), FHWA, and PB experts, regarding structural vulnerability include:

- Bridges and tunnels cannot be fully protected against significant disruption to roadway decks from even modest explosive quantities.

- Significant damage to the substructure of smaller bridges is to be expected with even modest explosive quantities. However, smaller bridges are not within the criteria used for “critical.” Conversely, larger bridges – including double-deck structures – are considered more likely targets.

- Larger bridges are less vulnerable by virtue of member size, spacing, redundancy, and ductility, including cables and hangers. Total collapse of single- or multiple-span bridges is less likely, although significant elements can be destroyed.

- Hinges and anchorages are special points of vulnerability, although access can be protected.

- On larger structures, roadway decks may experience considerable local damage – but can usually be repaired in a relatively short timeframe. Furthermore, decks may be considered “sacrificial” as they can provide significant protection to below-deck superstructure and substructure elements that may otherwise be breached. The exception is the case of cable-stayed and segmental box girder bridges, where the deck is an integral part of the structure.

- Hollow piers and below-deck substructure – depending on size and location – are vulnerable to proximity attacks, unless they have been designed for vessel ramming lateral impacts.

There are also significant differences in vulnerabilities by structure type:

- On larger suspension and cable-stayed bridges, cables, hangers, and main deck beams are relatively resistant to standoff blasts and fragments; collapse would occur only if multiple elements failed.

- Above-deck towers and hollow piers and box girders are vulnerable to proximity blasts, but protection and strengthening is presumed feasible. Bents and columns
on critical structures are usually large enough and include connections capable of withstanding substantial explosive forces.

- Above-roadway deck superstructures in through-deck truss and arch bridges are vulnerable to above deck lateral forces – especially on smaller structures.

- Newer bridges with piers in navigable water may already have been designed to withstand accidental ramming and thus are resistant to explosive attacks.

- Tunnels – including immersed tubes – are relatively invulnerable to blast-induced collapse or breeching, although internal fireballs and blast pressures will cause casualties and significant damage to decks and walls.

3.5 Bridge and Tunnel Countermeasures and Costs

Current military and engineering judgment indicates that complete protection from destruction of key structural elements is not feasible or cost effective. The countermeasures strategy must therefore include elements that focus on the DOD-based “4-D” approach:

- **Deter** attacks by the possibility of exposure, capture, or failure due to visible countermeasures.

- **Detect** potential attacks before they occur and provide the appropriate response force.

- **Defend** the asset by delaying and distancing the attacker from the asset and protecting the asset from the effects of weapons.

- **Design** (redesign) the asset to minimize the potential effects of WMD and conventional explosives.

These strategies, while focused in this report on asset protection, also have important life-saving benefits because they reduce the potential of significant damage to structures and facilities, as well as the attractiveness of the targets to threats.

The overall practical objective of the counter-terrorism measures is not to provide full protection of the assets, but to encourage terrorists to look elsewhere for easier targets (displacement) that will most likely involve less critical assets. Countermeasures, therefore, focus on:

- **Maximizing standoff distance** to key structural members via changes in land-use (relocation of parking, park use, etc.) and installation of various types of barriers at abutments and piers adjacent to above-roadway deck superstructures in through-deck truss and arch bridges.
• Denial of access to locations that would otherwise allow manual placement of explosives at points of structural vulnerability.

• Minimizing time-on-target for terrorists to undertake strategic placement of multiple time-coordinated detonations by using illumination surveillance cameras, real-time intrusion detection devices, and an active security patrol response.

• Selective upgrade of key structural members by strengthening may be feasible within the live- and dead-load limits of the structure. These might include the strengthening of key connections, modifications of hinges, and additions of stiffening elements to key members. Some of the features of earthquake-resistant design (e.g., ductility, connection details, redundancy, load redistribution, carbon fiber-reinforced polymer wrapping) are also applicable in blast-resistant design.

• Reduction of access to mechanical systems that introduce threats to personnel, e.g., infiltration of tunnel vents by biological and/or chemical agents and to areas that might compromise bascule or drawbridge operations should be considered.

• Coordination with local law enforcement through the use of automated detection and surveillance equipment, regular patrols and pre-planned routines for intrusion detection, and response to actual incidents.

Table 8 below summarizes countermeasures for bridges and tunnels.

Table 8: Bridge and Tunnel Countermeasures

<table>
<thead>
<tr>
<th>Strategy</th>
<th>Countermeasures</th>
</tr>
</thead>
</table>
| Defend: Increase standoff distance from bridge substructure and tunnel entrances | • Place barriers around ground approaches to below-deck piers/substructure  
• Place barriers to above-deck tower approach where feasible  
• Barricade/lock cable anchorage  
• Eliminate incompatible land-use, e.g., parking, parks, and other approaches to bridge or tunnel |
| Defend: Increase approach/ramming standoff from bridge piers in navigable water | • Fenders/dolphins for standoff waterway approaches if feasible |
| Deter and Detect: Monitor access to bridge substructure and tunnel portals | • Automated intrusion alarms, e.g., motion, infrared, and CCTV surveillance with tie-ins with traffic operations centers and local law enforcement for intrusion and incident response  
• Automated intrusion detection and tie-ins with manual surveillance  
• Institute regular patrols  
• Improve lighting  
• Lock out access to key structural elements |
### Strategy

| Design: Protect vent intakes in transverse/semi-transverse vent systems | - Relocate/extend and “fence-box” vent intakes to non-accessible locations |
| Design: Harden key structural elements | - Blast deflectors to shield towers  
- Strengthen/shield key above-deck members  
- Enhance connection details  
- Improve ductility and redundancy  
- Limit or confine damage |

### Bridge-Related Retrofit Costs

Table 9 below presents the capital costs for the above countermeasures as applied to the 451 critical bridges. The table includes costs for retrofit of all of the existing critical bridges, as well as special increments for bridges with piers in navigable waterways and highly visible bridges. Security-related cost increments associated with the condition-related reconstruction of critical bridges is discussed separately below.

#### Table 9: Six-Year Total Costs for Bridge Retrofit

<table>
<thead>
<tr>
<th>Countermeasure</th>
<th>Cost for 451 Critical Bridges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Above-deck tower protection (blast shielding)</td>
<td>$12M</td>
</tr>
<tr>
<td>Above-deck member strengthening/shielding</td>
<td>$39M</td>
</tr>
<tr>
<td>Lighting (above and below deck)</td>
<td>$40M</td>
</tr>
<tr>
<td>Intrusion detection &amp; surveillance (including CCTV)</td>
<td>$180M</td>
</tr>
<tr>
<td>Below-deck barriers &amp; fencing and/or pier wrapping (steel or FRP (fiber-reinforced polymer)) for strengthening</td>
<td>$87M</td>
</tr>
<tr>
<td>Navigable waterway bridge pier protection (40% of piers)</td>
<td>$139M</td>
</tr>
<tr>
<td>High visibility bridge above-deck member strengthening</td>
<td>$132M</td>
</tr>
<tr>
<td>Miscellaneous costs (20%)</td>
<td>$126M</td>
</tr>
<tr>
<td>Maintenance of traffic and contingencies (30%)</td>
<td>$225M</td>
</tr>
<tr>
<td>Total Capital Cost</td>
<td>$980M</td>
</tr>
<tr>
<td>Annual O&amp;M</td>
<td>$110M/Yr</td>
</tr>
</tbody>
</table>

For the aggregate estimate of basic security measures retrofit, the costs were developed through the application of unit costs for individual countermeasures as applicable to each of the three classes of bridges by structure type, i.e., suspension and cable-stayed, through and non-through deck truss and arch bridges, and girder bridges. Unit costs were applied based on aggregate length of bridges and number of piers for bridges identified as critical in each of the three bridge type categories. Basic bridge information was derived from the National Bridge Inventory. Unit costs are based on...
current analogous experience such as seismic retrofit and on-going state DOT security programs. The retrofit capital costs were allocated over the first four years of the Reauthorization period. The relationships between vulnerability and appropriate countermeasures are necessarily limited to generic characteristics of the asset type – without particular bridge and/or site-specific characterization. Significant contingency/uncertainty factors are included in recognition of the preliminary nature of these estimates. No adjustment has been made for the fact that some of these structures have already received initial treatment, such as fencing and CCTV monitoring, consistent with the measures assumed in this program strategy.

Operations and maintenance costs are based on 15 percent of cumulative installed security features on an annual basis.

Basic countermeasures were assumed to apply to all critical bridges, including:

- **Fencing**: Barriers to on- and off-ground approaches to below-deck piers/substructure, e.g., use of jersey barriers, chain link, and razor wire on land-side approaches to bridges and tunnels, and elimination of incompatible land-uses, e.g., parking, parks, and other approaches.

- **Lighting**: Illumination of vulnerable areas above and below decks.

- **Security patrols**: Active patrolling in response to elevated threat level warnings.

- **Bridge detection and surveillance**: Integrated intrusion detection/surveillance package for below-deck abutment and piers that may combine a selection of features including:
  - User-activated (at bridge or central TMC) pan/tilt CCTV cameras for verification;
  - Automated detection alarm system triggered by probable human or other non-routine presence, e.g., a mechanical robotic device that might include motion and/or heat (infrared) detectors focused on pier caps with the ability to discriminate between human and other intruders, such as birds and other animals;
  - Redundant communication systems with anti-jamming capability;
  - Connection of the surveillance systems at the bridge to a regional transportation management center staffed 24x7; and
  - Direct links to state and local law enforcement and the U.S. Coast Guard (USCG).

- **Lockout**: Barricade and/or locks applied to cable anchorages and other sensitive structural elements such as box girders, piers, and inspection platforms.

- **Barriers**: Separation of roadway-based, above-deck tower approaches where feasible, including devices to create vehicle standoff, such as bollards.
• **Member reinforcement**: In locations where pier standoff is not achievable by barriers, steel, or fiber-reinforced polymer (FRP) wrapping laminates to strengthen piers.

• **Tunnel vent protection**: Tunnel ventilation inducts extended and/or enclosed with locked wire box with heat/motion detection and CCTV surveillance.

• **Coordination with law enforcement**: The development of security-oriented detection and surveillance implies the importance of developing pre-planned coordinated incident-response protocols with local and state law enforcement entities including shared alarms and video and direct communications links. Maritime and riverine bridge and tunnel settings relating to major navigable waterways will require corresponding relationships with the USCG. Table 9 includes the cost of interconnecting bridge detection and surveillance systems with statewide emergency management/transportation management centers for each state in Years 2 and 3 of the Reauthorization period.

Certain countermeasures were assumed to apply only to special classes of bridges and were costed separately:

• **Special protection for “recognizable” structures.** Bridges and tunnels that were both critical and recognizable, estimated at five percent of critical bridges and 10 percent of critical tunnels, were assumed to receive additional treatment protecting above-deck structural members for bridges (on a total aggregate bridge length basis) and increased surveillance per tunnel. Where barriers cannot provide standoff, sacrificed energy-absorbing panels shielding may be considered at least until future research provides a more definitive approach.

• **Special protection for bridges over navigable waterways.** The large number (141) of critical bridges over navigable waterways, such as rivers, harbors, and estuaries, creates a special challenge. Ramming and explosives represent the major threats. Protection against deliberate ramming, e.g., using hijacked barges, overlaps with the problem of accidental ramming by errant barges. Dolphins that can deflect standard barges are increasingly in use on the navigable channels. In addition, accidental ramming is a well-known risk. Design specifications, i.e., AASHTO Load and Resistance Factor Design, have been available for 15 years. These specifications provide design guidance for at-risk piers, depending on the probability of collision and structural configuration. However, defense against placement of explosives, for example, by small boat or scuba, against in-water piers introduces a quite different design challenge. In-water fencing, while not impenetrable, may keep intruders at an acceptable standoff distance for a longer period of time; this, in combination with surveillance, may provide a valuable increase in security and cost considerably less than dolphin-type protection against accidental ramming. While an in-water bottom or pier-anchored fence device will introduce maintenance burdens, this may be an acceptable cost in “critical” contexts. For purposes of this cost estimate, it is assumed that 40 percent of the piers on critical bridges over 15 years old that span...
navigable waters and are potentially approachable directly from the water are so equipped.

**Bridge Reconstruction Costs**

New bridge construction and bridge rehabilitation, particularly the latter, occur constantly. Major reconstruction offers an opportunity to achieve a higher level of security as part of an otherwise scheduled activity. Assuming an average life span of 50-75 years, some major rehabilitation/reconstruction activities within the critical inventory would be expected. At present, approximately 70 percent of ongoing bridge construction activity is replacement and rehabilitation; there are few new major bridges being built. For purposes of this study, it is assumed that the larger bridges in the critical inventory absorb 10 percent of total expenditures.

For these critical bridges, a series of counter-terrorism design criteria may be developed through future research. These features would then be integral to the major bridge reconstruction projects in the critical inventory. Such features are assumed to include both layout considerations, such as pier placement to increase standoff distance from roadways as well as blast survivability design. The marginal cost of these design modifications is assumed to be 20 percent of total bridge reconstruction costs and allocated over each year of Reauthorization. A related operations and maintenance cost of 15 percent of the installed security improvements is also included. These costs are reflected in Table 9.

**Tunnel-Related Protection Costs**

Tunnels are relatively robust and invulnerable to serious damage, i.e., collapse, by personal or vehicle-mounted explosives, although tunnel linings and decks can experience significant damage causing closure. Tunnel portals can be closed from blast-induced rock falls and portal structure damage, but such damage is relatively easy to clear and repair. Therefore, internal tunnel protective measures are not assumed to go beyond contemporary NFPA fire and blast-related standards and costs related to bringing all major tunnels up to these standards. Most tunnels defined as critical are assumed to be meeting NFPA standards.

The 20 percent subset of critical tunnels assumed to be “critical and recognizable” were singled out for special protection including enhanced detection and surveillance (possible explosive detection, when available), as well as ventilation “lock boxes” to create standoff distance from intakes. Unit costs for enhanced surveillance and detection, as well as lock box construction, were applied to the 10 tunnels. Table 10 below presents the cost assumptions for tunnel protection. Table 5, Annual and Six-Year Total Costs Summary for Highway-Related Security Programs, presented previously, incorporates these costs, assumed to be incurred in Years 2 and 3 of the Reauthorization period.
<table>
<thead>
<tr>
<th>Countermeasure</th>
<th>Cost for 54 Tunnels</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bringing critical tunnels up to NFPA standards</td>
<td>No costs assumed</td>
</tr>
<tr>
<td>Critical tunnel (10) detection &amp; surveillance &amp; ventilation protection</td>
<td>$60M</td>
</tr>
</tbody>
</table>

3.6 **Needed Research Program**

While considerable materials are available regarding vulnerability and protective measures for building, a major research and development (R & D) program is required for bridges and tunnels. Such a program must include more systematic and detailed approaches to vulnerability and consequence analysis, risk management, and facility-specific countermeasures. There is the need for empirical as well as analytical material oriented towards bridges and tunnels to better understand explosive effects, blast phenomenology, blast-structure interaction, and the efficacy of various protective measures related to highways and bridges.

Design materials are available to address each of these areas, but many are in Department of Defense (DOD) publications and are no longer openly available. Furthermore, most of the DOD expertise has been focused on the effects of military munitions – not vehicle and other bomb threats. Simplified approaches, such as parametric studies and design guidelines, are needed to guide short-run structural retrofit programs.

The costs of such a research program have not been directly included, but a significant multiyear R & D program – drawing on both DOD and civil engineering resources – is needed. Because such a program is well beyond the normal capacity of state and academic resources, strong federal support would be required.

4. **Program for Enhancement of Traffic Management Capabilities**

Improving the capabilities of the urban roadway system to support terrorism-related emergency response and management – with regard to either on- or off-road events – is a key component of the national highway-related security program. Such a program is consistent with the Intelligent Transportation Systems (ITS) initiatives already underway in metro areas around the country.

4.1 **Needed Capabilities**

Current nationwide ITS initiatives are focused primarily on traffic and incident management along freeways and expressways and, to a lesser extent, signalized principal arterials. However, a range of special traffic operations regimes was needed in the immediate aftermath of the events of 9/11 in Lower Manhattan and Washington, DC/Arlington, Virginia. Several of these regimes are similar to those needed in natural and industrial disaster settings such as:
• Evacuation of population in the immediate area of an incident.

• Traffic management of highway-related incidents or from off-road incidents that “spill over” onto the highway infrastructure.

• Emergency access to the site of an incident.

• Bypassing affected/contaminated areas.

• Quarantining of affected/contaminated areas.

• Responding to the impacts of restrictions in site access under heightened security that may create new traffic patterns and related incidents.

The ability to provide these functionalities depends on the capacity of the system owner-operators – typically state DOTs and local governments – to actively manage and operate significant components of the regional roadway in real time. The management and operational needs include the capability to:

• Maximize traffic flow in one direction on major facilities.

• Restrict certain routes (perhaps multiple facilities) to specific vehicle types.

• Monitor current traffic flow, e.g., volume and speeds.

• Survey for incidents from camera locations and TMCs.

• Communicate with drivers.

4.2 Highway Management Systems Deployment

These abilities, in turn, require that these agencies have equipped the roadway with the necessary operational systems and established an integrated regional operational facility such as a traffic management center. In effect, this is the equivalent to a package of ITS and systems operations components that is increasingly standard in many major metropolitan areas. The standard components include:

• Automated vehicle detection technology to track system use, performance, and incidents.

• Surveillance systems to observe incidents and other problems from DOT operations and emergency management centers.
Variable message signs on principal routes to guide users regarding evacuation, emergency procedures, and routes.

These ITS systems for traffic management are typically operated from regional traffic management centers from which traffic is automatically monitored for incidents via automated roadway detection and in response to driver cell phone calls. Incidents are viewed via closed circuit TV (CCTV), variable message signs – activated remotely – display the appropriate messaging, and incident responders (e.g., fire, police, and traffic operations) are dispatched to the scene.

In some locations, hurricane and other major (and predictable) emergencies add additional dimensions to the existing regional emergency operations, including:

- Permanent fixed-route evacuation signing.
- Designation of pre-established reception centers.
- Broadcast of standard warnings and instructions.

To provide the necessary terrorism-related emergency management regimes described above, the ITS and emergency management traffic operations components need to be consistently applied in combination across the key roadway networks, especially in (but not limited to) major metropolitan areas. For purposes of this estimate, the 78 largest metropolitan areas (over 550,000 in population) have been included, although similar programs are also appropriate for key non-urban and intercity contexts. The overlap of security needs with other emergency management and congestion-related operational needs support an inclusive approach to definition of a logical network for improvement.

Deployment is assumed to be restricted to major facilities and those that carry significant traffic. Both access-controlled facilities, i.e., freeways/expressways and signalized principal arterials are included in these metropolitan networks. On the 78 metro area basis, this network incorporates about 10,500 miles of freeways/expressways and approximately 16,000 miles of principal arterials with a current volume/capacity ratio (V/C) of over 0.5. An additional 1,800 route miles is included to reflect nine STRAHNET “fort-to-port” connector routes supporting the most highway-dependent military installations.

Approximately 25 percent of the nation’s freeway network in the 78 largest metropolitan areas has already received traffic monitoring and surveillance systems deployment. The prospective security program would upgrade the remaining major network components in the largest metropolitan areas, providing the ability to monitor traffic conditions, view major incidents, and communicate with users in the event of major incidents or emergencies.
4.3 Highway Management Systems Strategic Control

The ability of the system to play one or more of the key roles (e.g., evacuation, emergency access, bypassing) in the most effective manner may depend on going beyond the reactive strategies typical of conventional traffic incident response operations. The focus and location of a terrorist event cannot be predicted; furthermore, the appropriate traffic management strategy will vary depending on the type of WMD involved and the scale of the action. In addition, some strategies involve consideration of destinations as well as origins (where traffic begins). Evacuation routes must ideally lead to reception centers; emergency access routes would typically lead to terrorist incident recovery sites.

Thus, emergency management makes additional demands on conventional traffic management and requires such extra functionalities as:

- Activation of systems on a corridor-specific or network-wide basis in response to the location of terrorist events.
- Incorporation of weather data to determine WMD plume effects (in cases of nuclear, biological, chemical, or radiological contamination and movement by winds) that affect routing decisions.
- Preprogrammed hazmat-specific response scenarios.
- The ability to respond to changing post-incident conditions such as hot spots and crime scene restrictions.
- Responsiveness to characteristics and capacities of reception centers.

The technology is rapidly becoming available to equip a traffic management center with these event-responsive, dynamic routing capabilities in real time and over large areas, drawing on national and regional databases, advanced mapping and imaging technology, and GIS (Geographic Information System)-based functionalities. For purposes of this estimate, it is assumed that the Office of Homeland Security (OHS) and other federal agencies, such as the Federal Emergency Management Agency (FEMA), the Transportation Security Administration (TSA), and the National Imaging and Mapping Agency (NIMA) would deploy these capabilities with the potential for both statewide and national control within several regional coordination centers covering multiple states.

Table 11 below presents the assumptions regarding coverage and treatments to develop the proposed systems.
### Table 11: Strategy Assumptions for National Highway Emergency Management and Monitoring System

<table>
<thead>
<tr>
<th>Location</th>
<th>Treatment</th>
<th>System</th>
<th>Coverage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Largest 78 Metropolitan Areas</td>
<td>• Remote traffic detection</td>
<td>• Interstate, freeways and other principal arterials</td>
<td>• Full coverage on high volume facilities (V/C &gt; 0.75)</td>
</tr>
<tr>
<td></td>
<td>• CCTV (medium scan)</td>
<td></td>
<td>• High incident locations on moderated volume facilities (V/C &gt; 0.5)</td>
</tr>
<tr>
<td></td>
<td>• Variable message signs (VMS) and other traveler information systems</td>
<td></td>
<td>• Spacing of cameras and detectors varies from 1-3 miles, VMS at 3-5 miles</td>
</tr>
<tr>
<td>STRAHNET</td>
<td>• Key fort-to-port routes</td>
<td>• Varies</td>
<td>1-10 miles</td>
</tr>
<tr>
<td>Data Integration</td>
<td>Urban (50) and statewide centers less those already installed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Regional Strategic Management Centers</td>
<td>Six regional centers (co-sponsored by federal and state agencies)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 4.4 Program Costs

The cost estimates in Table 12 below are based on spacing assumptions and unit costs developed for FHWA and modified by current ITS deployment experience.

### Table 12: Six-Year Total Costs for Enhancement of Traffic Management Capabilities

<table>
<thead>
<tr>
<th>Strategy</th>
<th>Coverage</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detection, surveillance and traveler information package</td>
<td>Largest 78 metro areas Freeways and Expressways with V/C &gt; 0.5 Arterials with V/C &gt; 0.5</td>
<td>$1,299M</td>
</tr>
<tr>
<td></td>
<td>Key STRAHNET routes Nine fort-to-port routes</td>
<td>$288M</td>
</tr>
<tr>
<td>New TMCs and data integration</td>
<td>31 new centers and upgrades to existing metropolitan or statewide centers</td>
<td>$315M</td>
</tr>
<tr>
<td>Regional strategic centers</td>
<td>Six multi-state regional centers</td>
<td>$60M</td>
</tr>
<tr>
<td>Total Capital Cost</td>
<td></td>
<td>$3,654M</td>
</tr>
<tr>
<td>Annual O&amp;M</td>
<td></td>
<td>$319M</td>
</tr>
</tbody>
</table>

The baseline installation of traffic management systems for emergency response would include three basic elements:
Automated vehicle detection technology to track system use, performance, and incidents. Such vehicle detectors are presumed increasingly to be non-intrusive technology, such as infrared or radar with pairs, on one-mile spacing on higher volume (V/C > 0.75) freeways and expressways, and intervals varying from three to five miles on principal arterials with V/C from 0.5 - 0.75, depending on configuration.

Surveillance systems, assuming medium bandwidth CCTV with pan/tilt/zoom (PTZ) capabilities on five-mile spacing to observe incidents and other problems from DOT operations and emergency management centers.

Over-the-roadway-mounted variable message signs on principal routes at five-mile intervals to guide users regarding evacuation, emergency procedures, and routes.

Unit cost estimates are all-inclusive, i.e., pole, cabinet foundations, power, modems, cameras, and communications lease.

The integration of data from these new systems is assumed to take place in metropolitan traffic management centers. Thirty-one modest new centers are assumed with some upgrades to handle data integration in the other 47 centers.

The new federal-state regional strategic coordination centers are assumed to be established on a multi-state basis (nine nationwide). They would bring national security community capabilities together with access to local transportation, geographic, and other data for dynamic emergency routing purposes. The costs for the regional strategic management capacity represent an order-of magnitude estimate of an appropriate share of a federal-state installation.

Annual operating costs are estimated at 15 percent of installed capital.

For purposes of this estimate, all capital and operating costs are assumed to be attributable to security. However, given the multipurpose potential of these investments for general traffic management, some proportion of the costs may be considered part of state DOTs “normal” commitment to systems management.

5. Program for Improvement of State DOT Emergency Response

This section describes the third “leg” of the overall recommended program for state departments of transportation to pursue after the events of 9/11. This strategy focuses on upgrading the emergency response capabilities of state DOTs.

Traditionally, state DOTs have been designated with specific transportation-oriented responsibilities in emergencies. The functions are typically set forth at a high level in the state emergency management plans and are often detailed in DOT emergency operations plans. These functions have been determined in anticipation of a range of
potential emergencies including natural disasters (e.g., hurricanes, floods, storms, and earthquakes) and technology-based disasters (e.g., hazardous materials spills, nuclear explosions, and biological incidents).

In recent years, state DOTs have been called to assist in the aftermath of terrorist incidents involving weapons of mass destruction. These agencies are likely to continue to play a role in the future if terrorists persist in attacking the United States; most likely, state DOTs will play a growing role.

5.1 Expanding Role of State DOTs in Emergency Response

State DOTs can and do play a significant role in emergency response for several reasons. A few are listed below:

- State DOTs have personnel distributed statewide on the highway networks who are in a position to observe and report unusual or suspicious behaviors, essentially providing “eyes and ears” across a large intermodal network.

- State DOT personnel are deploying more employees who are trained to respond to incidents, e.g., safety service patrols, and DOT personnel could well be the first responders on the scene after a terrorist incident.

- State DOTs are improving their incident management capabilities, and these can lend themselves to terrorist incident response.

- State DOTs frequently have extensive statewide communications networks that are used in times of crisis.

- State DOTs have the capability to provide detection, surveillance, and monitoring over the highway network and, in some cases, nearby areas.

- State DOTs often provide the heavy equipment necessary to remove large debris after terrorist incidents.

- State DOTs are often one of the largest agencies in most states and can provide substantial numbers of personnel, including engineers, to response efforts.

- State DOTs have the expertise to route, divert, restrict, or otherwise direct traffic after terrorist incidents, and are instrumental in developing emergency routes for egress or ingress to affected areas.

- State DOTs are increasingly focused on operations (vis-à-vis construction) and thus are improving their skills in overall system management, which is critical for response efforts.
If state DOTs are to play expanded roles in the response to future terrorist incidents, their emergency management and response capabilities must be enhanced.

5.2 Fundamental Emergency Management Thinking

Some fundamental principles underlie today’s emergency management thinking. These include:

• Public agencies that have to address significant emergencies should have an emergency management plan(s) in place.

• Those agencies that face a range of emergencies, e.g., natural or human-caused, should develop an all-hazards approach, meaning that the same fundamental approach should be taken to address all types of emergencies. However, some emergencies may require a modified or expanded approach. In those instances, additional annexes are often added to the basic emergency management plan. Plans specific to terrorism are typically found in an annex.

• Agencies should view emergency management as a cycle of four related components:
  o Mitigation: Steps taken in advance to reduce the potential loss from a hazard.
  o Preparedness: Steps taken in advance to facilitate the response and recovery after a hazard event.
  o Response: Steps taken during, or immediately after, a hazard event to save lives and property.
  o Recovery: Steps taken to restore the affected areas to their normal status. During the course of recovery, mitigation steps should be considered to reduce the future consequences of a similar hazard event.

• Typically, most response agencies use the Incident Command System (ICS). This system provides responders with a flexible tool for directing, controlling, and coordinating resources dedicated to incident response. The ICS applies a common organizational structure that can be contracted or expanded as the response effort changes in nature. It also provides a common set of management principles to help standardize response efforts. The concept of Unified Command is often associated with ICS. Unified Command involves enabling all agencies with responsibility for the incident to help manage an incident by establishing a common set of incident objectives and strategies. While most common in the law enforcement and fire communities, the application of ICS and Unified Command concepts has broad application, e.g., to a state DOT incident management program.

Many state DOTs have acted on these fundamental emergency management principles. However, most, if not all, DOTs need to examine needed changes after 9/11 and create or modify existing plans and put into effect a variety of other programmatic changes to enhance emergency response. These changes will have a significant impact on state DOT budgets.
5.3 Identified Shortcomings

Traditionally, state DOTs have provided support functions in the existing emergency plans of state emergency management agencies. These “all-hazard” statewide plans have proven to be robust tools for natural disasters. However, the 9/11 experience has indicated the need to continuously update and modify these statewide plans, including the supporting emergency operations plans of the state DOTs. Many state DOTs are currently in the process of updating their emergency operations plans. Some are preparing these plans for the first time. The DOTs are generally also working closely with their state emergency management agencies to better adapt the statewide plans to the challenges of terrorism.

Past terrorist incidents have led to the identification of several important challenges, including:

- **Absence of interoperable and reliable communications among agencies.** The combination of system overloads, destruction of communication lines and centers, and incompatible technologies among public safety and transportation agencies emphasizes the dangers inherent in institutional isolation. A concerted effort to develop robust and interoperable communications systems for both data and voice are an essential component of improved emergency response – as well as key to improved incident management in general.

- **Lack of familiarity with the role and personnel of other agencies.** Paper protocols are no substitute for face-to-face familiarity with agency partners where unanticipated circumstances call for quick, on-the-scene cooperative judgments and action. Joint training and regular exercises are an essential and continuing requirement for maximum effectiveness.

- **Responding to the introduction of federal security agencies and crime scene factors.** Terrorist incidents – by law – introduce federal security agencies with specific priorities into the incident command context. The site of the terrorist act may be treated as a crime scene with special access restrictions. Federal agents and the military may require the use of on-scene communications; this was the case when the Virginia Department of Transportation (VDOT) control center adjacent to the Pentagon became a military command center on 9/11.

- **Unfamiliarity with Incident Command System (ICS) practices of public safety agencies.** Public safety agencies in charge of the 9/11 response utilized an incident command structure as they do for most major incidents. This approach clarifies the chain of command and allocates key responsibilities. Not all transportation agencies are knowledgeable about, or experienced in using, ICS.

- **Need for specific operations regimes such as evacuation and emergency access.** Public reaction in both New York and Washington, DC on 9/11 included a large amount of self-evacuation as people strove to leave the affected areas and unite
with their families. In both the New York and Washington, DC areas, multi-modal transportation resources were mobilized in an ad-hoc fashion to accommodate these demands. At the same time that large numbers of people were trying to leave the impacted areas, there was also a need to bring trained personnel, supplies, and equipment to those areas. The need for a more organized approach to evacuation and emergency access, e.g., the identification of critical emergency routes, was clearly demonstrated.

- **Protection of first responders from biological, chemical, and radiological hazards.** The history of terrorist incidents suggests the need for more attention to the protection of first responders including their ability to recognize threat types to avoid hazards, and to avail themselves of personal protection equipment, hazard detectors, and decontamination facilities. Terrorist access to a broader range of weapons indicates the need to consider a wider range of hazards.

- **Capitalizing on Intelligent Transportation Systems (ITS) technology for traffic control and communications.** In New York, the Transportation Operations Coordinating Committee (TRANSCOM) multi-agency communications capability proved its value in keeping multiple agencies up-to-date regarding post-incident travel conditions. At the same time, ITS traffic management features were used to accommodate the need for reverse flows and special emergency access in and out of Manhattan and the Washington, DC area.

These challenges need to be addressed by state DOTs as part of enhancing their emergency response capabilities. State DOTs must also explain and apprise state emergency managers of potential roles the DOTs might perform. For example, the use of ITS and the enhanced capabilities for detection, surveillance, and monitoring might be better utilized by state emergency managers. These capabilities could also be better tied to law enforcement information systems allowing more robust abilities to identify potential or actual terrorist activities or incidents. Systems such as the Capital Wireless Integrated Network (CapWIN) in the Washington, DC area hold promise for the improved sharing of data between transportation and law enforcement agencies.

Transportation strategies embodied in existing plans may need to be adjusted for characteristics such as scale, additional responder risks, crime scene management, and other factors related to the use of WMD. The need for special transportation responses, e.g., evacuation, quarantining, etc, may be introduced. A set of new hazards for first responders must be a consideration. These and other issues suggest the need to consider appropriate modifications and/or improvements that may be appropriate to the WMD context.

State DOTs can also look to practices and experiences that can provide guidance for emergency response to terrorist incidents, including, for example:

- Standard emergency management.
• Incident management (as already applied by many highway agencies).
• Planning for non-terrorist, technological disasters, e.g., Y2K and nuclear power plant evacuations.
• Planning for natural disasters, e.g., hurricanes, earthquakes, and floods.
• Lessons learned from 9/11 and other terrorist incidents (such as those listed previously).

5.4 An Emergency Response Capacity-Building Program for State DOTs

In order to remedy the identified shortcomings in state DOT emergency management practices, a general capacity-building program to improve emergency response capabilities has been targeted to an “average” state DOT. The components are described in Table 13 below:

<table>
<thead>
<tr>
<th>Program Sub-Elements</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Program Development, Management, &amp; Oversight</td>
<td>• Develop Modified or New Programs&lt;br&gt;• Direct &amp; Oversee Planning, Training, Exercising, &amp; Public Information&lt;br&gt;• Coordinate Diverse Stakeholders (internal &amp; external to state DOT)&lt;br&gt;• Develop Budgets&lt;br&gt;• Procure Services&lt;br&gt;• Manage Emergency Response Personnel&lt;br&gt;• Manage Consultants &amp; Contractors</td>
</tr>
<tr>
<td>Planning (to assess general response needs &amp; requirements)</td>
<td>• Emergency Operations Plans&lt;br&gt;• Critical Asset Identification&lt;br&gt;• Vulnerability Assessment &amp; Countermeasures&lt;br&gt;• Threat Analysis&lt;br&gt;• Hazards Analysis&lt;br&gt;• Evacuation Planning&lt;br&gt;• Traveler Information&lt;br&gt;• System Surveillance &amp; Monitoring&lt;br&gt;• Asset Management&lt;br&gt;• Communications</td>
</tr>
<tr>
<td>Training (for awareness &amp; more advanced response)</td>
<td>• Develop Training&lt;br&gt;• Deliver Training</td>
</tr>
<tr>
<td>Exercising (for testing &amp; practicing actual response readiness)</td>
<td>• Develop Exercises&lt;br&gt;• Deliver Exercises</td>
</tr>
<tr>
<td>Public Information (for response to public concerns &amp; needs in an emergency)</td>
<td>• Develop Coordinated Strategies</td>
</tr>
<tr>
<td>Program Sub-Elements</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Systems-Specific Planning</td>
<td>• Traveler Information Systems&lt;br&gt;• System Surveillance &amp; Monitoring Systems&lt;br&gt;• Communications Systems&lt;br&gt;• Other Systems-Related to Emergency Routes&lt;br&gt;• Response Assets Management Systems</td>
</tr>
<tr>
<td>System Construction</td>
<td>• Expanded or New Communications Systems&lt;br&gt;• Other Communications Upgrades</td>
</tr>
<tr>
<td>Operations &amp; Maintenance</td>
<td>• Communications Systems&lt;br&gt;• Additional Security Guards&lt;br&gt;• Carrying Cost of Additional Equipment and Supplies&lt;br&gt;• Personal Protective Equipment</td>
</tr>
</tbody>
</table>

Below is some additional explanation of the program sub-elements.

- **Program Development, Management, & Oversight**: This program sub-element relates to the development of new programs for enhanced security and emergency response and their continuing management and oversight by state DOT personnel. This cost category consists entirely of state DOT personnel costs. While many state DOTs will try to use existing personnel to perform new security and emergency response functions, there will be a need to bring on personnel with different skill sets. Regardless of whether a number of new personnel are hired, there is a cost to the organization for the new security and emergency response programs, whether new hires or diversion of existing staff. This cost should be recognized. This program sub-element also covers – at least in part – the state DOT personnel time devoted to the sub-elements below such as planning and training.

- **Planning, Training, Exercising, and Public Information**: These program sub-elements are grouped because they all have to do with readying state DOTS for effective emergency response when an incident occurs. In contrast to the Program Development, Management, & Oversight sub-element, costs incurred in these sub-elements, for purposes of this study, are assumed to be those for consultants and/or contractors. These will be experts to assist state DOTs in a range of activities including planning activities as listed in the above table, the development and delivery of training and exercises, and assistance in developing public information strategies. Some state DOTs will choose to use outside assistance in all of these areas and some in just a few, depending on the availability of in-house personnel and financial resources.

- **Systems-Specific Planning**: Unlike the general emergency management planning described above, this program sub-element refers to planning and design for specific systems that are beneficial for emergency response. These could be the systems to provide surveillance and monitoring for bridges as well as the systems to support the second program (see Part II, Section 4, Program for Enhancement of Traffic...
Management Capabilities). Planning for effective communications systems would also be included here.

- **Communications**: In Sections 3 and 4, the major capital costs associated with state DOT security programs were defined, including infrastructure countermeasures and highway emergency management systems. This sub-element focuses on the necessity for robust, redundant, and interoperable communications during response to a significant incident. The states and state DOTs are in different stages of progress in their development of communications systems. Some have sophisticated radio systems that fully enable statewide coverage; others have antiquated radio systems with limited coverage or other problems. Interoperability between the various state communications systems is often lacking. Funding for statewide systems can cost several hundred million dollars, while a state DOT system can cost in the tens of millions. Spectrum availability is also an issue. The costs related to the construction of communications systems are primarily assumed to be those for hardware, software, and consultant/contractor time.

- **Other Operations and Maintenance**: This program sub-element includes non-capital costs of such items as maintaining communications systems and the cost of additional security guards to observe and guard certain critical assets such as TMCs. For purposes of this study, many of these costs are assumed to be incurred by consultants and/or contractors working for state DOTs, e.g., security guards. The cost of personal protective equipment is also included because it is a relatively low cost item in small quantities. Note, however, that the costs can quickly rise if purchased in-bulk.

### 5.5 Program Costs

For purposes of determining the cost of an emergency response capacity-building program, both capital and operating costs are calculated over the six-year period of the next Federal reauthorization legislation. It is envisioned that many of the improvements state DOTs need to make will be made over that six years. However, given the ramp-up in emergency management and response activities, additional costs will accrue in the years beyond the next reauthorization, e.g., increased operating costs for deployed surveillance devices. Costs have been calculated based on discussions with state DOTs and other experts.

Some of the investments from this program area will provide benefits beyond response to terrorist incidents alone. For example, a portion of the investment will enhance state and state DOT efforts to better respond to natural and industrial disasters. In addition, updated and/or new communications systems can be utilized for a range of day-to-day management and operations purposes. These improvements will provide dividends for the long term.

The cost of building emergency response capacity in state DOTs is shown in Table 14, below:
Table 14: Annual and Six-Year Total Costs for Improvement of State DOT Emergency Response Capabilities

(Note: Costs are in millions)

<table>
<thead>
<tr>
<th>Program Sub-Elements</th>
<th>Cost Type</th>
<th>Year 1</th>
<th>Year 2</th>
<th>Year 3</th>
<th>Year 4</th>
<th>Year 5</th>
<th>Year 6</th>
<th>Total Capital Costs</th>
<th>Total Operating Costs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Program Development, Management &amp; Oversight</td>
<td>Capital</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
</tr>
<tr>
<td></td>
<td>O&amp;M</td>
<td>$52</td>
<td>$52</td>
<td>$52</td>
<td>$52</td>
<td>$52</td>
<td>$52</td>
<td>$312</td>
<td></td>
</tr>
<tr>
<td>Planning</td>
<td>Capital</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>O&amp;M</td>
<td>$78</td>
<td>$46</td>
<td>$19</td>
<td>$18</td>
<td>$18</td>
<td>$18</td>
<td>$197</td>
<td></td>
</tr>
<tr>
<td>Training</td>
<td>Capital</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>O&amp;M</td>
<td>$33</td>
<td>$2</td>
<td>$2</td>
<td>$2</td>
<td>$2</td>
<td>$2</td>
<td>$43</td>
<td></td>
</tr>
<tr>
<td>Exercising</td>
<td>Capital</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>O&amp;M</td>
<td>$23</td>
<td>$23</td>
<td>$23</td>
<td>$23</td>
<td>$23</td>
<td>$23</td>
<td>$138</td>
<td></td>
</tr>
<tr>
<td>Public Information</td>
<td>Capital</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>O&amp;M</td>
<td>$3</td>
<td>$3</td>
<td>$3</td>
<td>$3</td>
<td>$3</td>
<td>$3</td>
<td>$18</td>
<td></td>
</tr>
<tr>
<td>Systems-Specific Planning (could be capital or O&amp;M funding)</td>
<td>Capital</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>O&amp;M</td>
<td>$78</td>
<td>$20</td>
<td>$9</td>
<td>$9</td>
<td>$9</td>
<td>$9</td>
<td>$134</td>
<td></td>
</tr>
<tr>
<td>Other Operations &amp; Maintenance</td>
<td>Capital</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>O&amp;M</td>
<td>$55</td>
<td>$50</td>
<td>$50</td>
<td>$50</td>
<td>$50</td>
<td>$50</td>
<td>$305</td>
<td></td>
</tr>
<tr>
<td>Communications System</td>
<td>Capital</td>
<td>$156</td>
<td>$156</td>
<td>$156</td>
<td>$156</td>
<td>$156</td>
<td>$156</td>
<td>$936</td>
<td></td>
</tr>
<tr>
<td></td>
<td>O&amp;M</td>
<td>$23</td>
<td>$47</td>
<td>$70</td>
<td>$94</td>
<td>$117</td>
<td>$140</td>
<td>$491</td>
<td></td>
</tr>
<tr>
<td>Yearly Capital/O&amp;M Costs Totals</td>
<td>Capital</td>
<td>$156</td>
<td>$156</td>
<td>$156</td>
<td>$156</td>
<td>$156</td>
<td>$156</td>
<td>$936</td>
<td></td>
</tr>
<tr>
<td></td>
<td>O&amp;M</td>
<td>$345</td>
<td>$243</td>
<td>$228</td>
<td>$251</td>
<td>$274</td>
<td>$297</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yearly Overall Totals</td>
<td>$501</td>
<td>$399</td>
<td>$384</td>
<td>$407</td>
<td>$430</td>
<td>$453</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Six-Year Totals</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$936</td>
<td>$1,638</td>
<td></td>
</tr>
</tbody>
</table>

5.6 Cost Analysis Assumptions

In the analysis of costs for enhanced emergency response, the following assumptions were made:
• Total number of state DOTs (52).

52 state DOTs are included in this analysis. This number is based on membership in AASHTO and includes the 50 state DOTs plus those from the District of Columbia and Puerto Rico.

• Average number of employees per state DOT (5,000).

The average state DOT was calculated to include 5,000 employees, based on two sources provided by AASHTO. The first source was the U.S. Census Bureau’s *Statistical Abstract of the United States, 2001*, which reflected a total of 246,200 full-time equivalent state employees in the functional area of highways. This number was divided by 50 to determine the average number of employees per state DOT, resulting in a number of 4,920 (Note: The District of Columbia and Puerto Rico were not included in the *Statistical Abstract* total so the total number of employees was divided by 50 rather than 52.). A second source was the 2001 AASHTO Salary Survey, which showed 228,766 employees across 45 state DOTs, resulting in a number of 5,083 (Note: Seven out of the 52 did not show their number of employees.). The average of 4,920 and 5,083 is approximately 5,000 employees.

• Average yearly state DOT salary with benefits and overhead ($100,000).

The average monthly state DOT employee salary was calculated to be $3,038 or $36,456 on an annual basis. This number is based on the 2001 AASHTO Salary Survey, which reflected an AASHTO monthly mean salary of $2,809. This 2001 number was adjusted upwards to reflect pay increases of four percent in 2002 and 2003. These pay increases were included since the period covered by the calculations in this report will not realistically begin until passage and implementation of the surface transportation reauthorization in 2003. For purposes of this report, full-time equivalent costs for supporting an employee, including salary, benefits, and organizational overhead, were estimated at $91,140. This was rounded to $100,000 per employee per year because much of the anticipated work to be performed by state employees would involve those who are more highly paid.

• Total number of years over which costs might be allocated (6).

The total number of years over which costs are calculated is meant to cover the likely six-year period of the pending federal surface transportation legislation.

• Operations and maintenance for capital projects.

Operations and maintenance costs are calculated as 15 percent of the installed capital base. In other words, if an 800 MHz radio communications system is built
out over three years, the first year’s O&M is calculated at 15 percent of the installed radio system, and the second and third years in the same way. Beyond the three years, i.e., after complete build-out, the O&M cost would be assumed to be the same as the third year’s for the fourth through sixth years covered by this study.
6. Appendix

A. List of Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>9/11</td>
<td>September 11, 2001</td>
</tr>
<tr>
<td>AASHTO</td>
<td>American Association of State Highway and Transportation Officials</td>
</tr>
<tr>
<td>ADT</td>
<td>Average Daily Traffic</td>
</tr>
<tr>
<td>ATF</td>
<td>Bureau of Alcohol, Tobacco, and Firearms</td>
</tr>
<tr>
<td>CapWIN</td>
<td>Capital Area Wireless Integrated Network</td>
</tr>
<tr>
<td>CCTV</td>
<td>Closed-Circuit Television</td>
</tr>
<tr>
<td>DOD</td>
<td>Department of Defense</td>
</tr>
<tr>
<td>DOT</td>
<td>Department of Transportation</td>
</tr>
<tr>
<td>FEMA</td>
<td>Federal Emergency Management Agency</td>
</tr>
<tr>
<td>FHWA</td>
<td>Federal Highway Administration</td>
</tr>
<tr>
<td>FRP</td>
<td>Fiber-Reinforced Polymer</td>
</tr>
<tr>
<td>GIS</td>
<td>Geographic Information System</td>
</tr>
<tr>
<td>ICS</td>
<td>Incident Command System</td>
</tr>
<tr>
<td>ITS</td>
<td>Intelligent Transportation Systems</td>
</tr>
<tr>
<td>MTMC</td>
<td>Military Traffic Management Command</td>
</tr>
<tr>
<td>NBI</td>
<td>National Bridge Inventory</td>
</tr>
<tr>
<td>NCHRP</td>
<td>National Cooperative Highway Research Program</td>
</tr>
<tr>
<td>NFPA</td>
<td>National Fire Protection Association</td>
</tr>
<tr>
<td>NIMA</td>
<td>National Imaging and Mapping Agency</td>
</tr>
<tr>
<td>O&amp;M</td>
<td>Operations and Maintenance</td>
</tr>
<tr>
<td>OHS</td>
<td>Office of Homeland Security</td>
</tr>
<tr>
<td>PB</td>
<td>Parsons Brinckerhoff</td>
</tr>
<tr>
<td>PBF</td>
<td>PB Farradyne</td>
</tr>
<tr>
<td>R&amp;D</td>
<td>Research and Development</td>
</tr>
<tr>
<td>SAIC</td>
<td>Science Applications International Corporation</td>
</tr>
<tr>
<td>STRAHNET</td>
<td>Strategic Highway Network</td>
</tr>
<tr>
<td>TCRP</td>
<td>Transportation Cooperative Research Program</td>
</tr>
<tr>
<td>TEA-21</td>
<td>Transportation Equity Act for the 21st Century</td>
</tr>
<tr>
<td>TMC</td>
<td>Transportation Management Center</td>
</tr>
<tr>
<td>TMS</td>
<td>Tunnel Management System</td>
</tr>
<tr>
<td>TRANSCOM</td>
<td>Transportation Operations Coordinating Committee</td>
</tr>
<tr>
<td>TSA</td>
<td>Transportation Security Administration</td>
</tr>
<tr>
<td>USACE</td>
<td>United States Army Corps of Engineers</td>
</tr>
<tr>
<td>USCG</td>
<td>United States Coast Guard</td>
</tr>
<tr>
<td>V/C</td>
<td>Volume/Capacity Ratio</td>
</tr>
<tr>
<td>VDOT</td>
<td>Virginia Department of Transportation</td>
</tr>
<tr>
<td>VMS</td>
<td>Variable Message Sign</td>
</tr>
<tr>
<td>WMD</td>
<td>Weapons of Mass Destruction</td>
</tr>
</tbody>
</table>